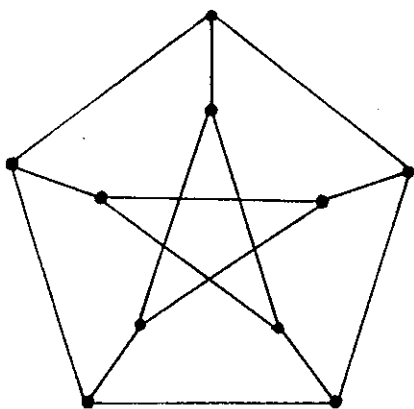


Aron Simis

# Combinatória Algébrica



O grafo de Petersen

*Ilustrou*

**Nora Simmetz**

ARON SIMIS

Instituto de Matemática

Univ. Fed. da Bahia

Av. Ademar de Barros, s/n

Campus Universitário da Federação

40000 – Salvador-BA

COPYRIGHT © by Aron Simis

Nenhuma parte deste livro pode ser reproduzida,  
por qualquer processo, sem a permissão do autor.

ISBN

85-244-0054-4

**Conselho Nacional de Desenvolvimento Científico e Tecnológico**

**INSTITUTO DE MATEMÁTICA PURA E APLICADA**

Estrada Dona Castorina, 110

22.460 – Rio de Janeiro-RJ

*Este livro é dedicado a Lu,  
pelo seu esforço olímpico,  
onde quase tudo é combinatória...*

*C'est de l'algèbre,  
ce dit d'une chose  
à laquelle on ne  
comprend rien.*

**Litré**



## PREFÁCIO

Meu objetivo com estas notas é introduzir uma área de desenvolvimento recente, ainda não suficientemente amadurecida no que se refere a métodos e resultados centrais, mas que goza de prestígio crescente junto a algebristas e especialistas em combinatória.

Mais precisamente, apresento resultados de interfaceamento entre partes da Combinatória e da Álgebra Comutativa, com ênfase na interpretação algébrico-geométrica de problemas oriundos da primeira.

Para usar de um conhecido *caveat*, não existe, no momento, tanto quanto saiba, um texto básico nesta área – muito menos, em português. De certa maneira, o texto de R. Stanley, *Combinatorics and Commutative Algebra* (Birkhäuser, 1983), tem servido como guia e roteiro para os especialistas. Contudo, os pre-requisitos para sua correta digestão variam desde exposições prévias a tópicos de Topologia Algébrica até um grau avançado de maturidade em Álgebra Comutativa, tornando o texto uma leitura árdua para o noviço.

Minha intenção original era a de evitar estes pre-requisitos, de modo que as estruturas combinatórias ficassem em evidência o mais cedo possível e o instrumento algébrico, quando estritamente necessário. À medida que me avizinhava dos resultados mais profundos, comecei a entender o drama de Stanley. Disfarçadamente, empurrei os pre-requisitos para o final das notas, na forma de uma *Terminologia* – enquanto Stanley os traz no início!

Mas, esta não é a única diferença. Certamente, um dos objetivos deste

curso é divulgar alguns dos resultados obtidos por Stanley. Existem, contudo, inúmeras facetas da combinatória algébrica que são igualmente dignas de menção, entre estas a teoria algébrica e matricial dos grafos, a teoria dos invariantes, a teoria das variedades tóricas e dos politopos que se associam, os arranjos de hiperplanos de Orlik–Terao, a teoria dos elementos finitos (“spline theory”) de Billera, desenho de blocos e a combinatória numérica dos ideais polinomiais.

Um critério de seleção que me pareceu adequado e que tentei seguir durante a preparação das notas, foi o de qualificar estruturas combinatórias que admitissem transferência não trivial para álgebra comutativa. Como sempre, o trabalho de execução é sempre mais monumental do que o plano original.

De qualquer maneira, seguindo o critério, a teoria dos grafos pareceu ter uma importância especial, a qual procurei destacar.

Como advertência ao leitor ávido pelos mais recentes desdobramentos da teoria dos grafos nas áreas tecnológicas, gostaria, contudo, de esclarecer que este não é um texto sobre aquela teoria. Não se trata sequer de um texto visando tornar a teoria digerível para o público matemático. O interessado nestas duas vertentes sofrerá, infelizmente, uma decepção.

Estas notas são de interesse puramente matemático; os tópicos, tratados de modo matemático, poderiam prescindir totalmente das representações dos grafos como figuras geométricas que obedecem a prescrições de incidência. Isto, entretanto, seria um pedantismo inútil, tornaria a compreensão das idéias lenta e irritante e privaria o leitor sem experiência anterior de um prazer estético comprovado.

Assim, o produto final é um caso de personalidade dividida: os primeiros capítulos dão a impressão de um livro sobre grafos – exceto pelo *intermezzo* que se ocupa de complexos simpliciais abstratos e dos politopos; os demais, apropriam-se devidamente da alcunha *Combinatória Algébrica*. A meio caminho, assim o espero, o leitor terá a sensação de um “perfect matching”.

Parte destas notas foram escritas durante uma visita do autor ao Max-Planck-Institut für Mathematik (Bonn, Alemanha) durante o primeiro semestre de 1991. Àquela Instituição, personificada pelo seu Diretor, Prof. F. Hirzebruch, e ao meu colega da Universidade de Köln, Prof. M. Herrmann, meus agradecimentos por terem provido ambiente estimulante para a feitura deste e de outros trabalhos.

ARON SIMIS

Departamento de Matemática  
Universidade Federal da bahia  
USERARON@LNCC.BITNET

Abril, 1991





	Prefácio . . . . .	i
<b>Capítulo 1.</b>	<b>Grafos, I: Generalidades</b>	
1.1	Grafos como relações . . . . .	2
1.2	Realização de grafos . . . . .	2
1.3	Grafos e seus automorfismos . . . . .	6
1.4	Subgrafos e árvores geradoras . . . . .	8
1.5	Coloração de vértices, grafos $r$ -partidos . . . . .	9
1.6	Conjuntos parcialmente ordenados . . . . .	10
<b>Capítulo 2.</b>	<b>Grafos, II: Complexidade</b>	
	Complexidade algorítmica	
2.1	Coberturas de vértices . . . . .	14
2.2	Conjuntos independentes . . . . .	18
	Complexidade simplicial	
2.3	Complexos simpliciais abstratos . . . . .	22
2.4	Politopos e $f$ -vetores . . . . .	24
2.5	Transferências combinatórias . . . . .	29
<b>Capítulo 3.</b>	<b>Álgebra Comutativa, I: O papel dos monômios</b>	
	Monômios: encarnações	
3.1	Monômios livres de quadrados . . . . .	36
3.2	Primeira encarnação: Hodge, álgebras discretas . . . . .	37
3.3	Segunda: Macaulay . . . . .	39
3.4	Terceira: Hironaka, Rees, outros . . . . .	41
	Aneis de faces e arestas	
3.5	O anel de Petersen . . . . .	46

3.6	O anel de Stanley-Reisner . . . . .	51
3.7	Série de Hilbert e $h$ -sequências . . . . .	54

**Capítulo 4. Álgebra Comutativa, II: O fato Cohen-Macaulay**

**Cohen-Macaulay, I**

4.1	Aneis de Cohen-Macaulay . . . . .	60
4.2	O teorema de Hochster-Reisner-Munkres . . . . .	69
4.3	A conjectura da cota superior . . . . .	73

**Cohen-Macaulay, II**

4.4	A suspensão de um grafo . . . . .	76
4.5	O pedestal e o tipo de um grafo . . . . .	82
4.6	Relações polinomiais . . . . .	84

**Apêndice. *Pentimento***

**Palimpsesto 1: Teoria dos**

**Invariantes . . . . . 101**

2.1 Variedades tóricas e politopos, *101*; 1.2 Bases de Gröbner, *105*

**Palimpsesto 2: Potências**

**simbólicas . . . . . 108**

2.1 Potências simbólicas e ciclos ímpares, *108*; 2.2 Número cromático versus potências simbólicas, *112*

**Palimpsesto 3: Computação**

**algébrica em Combinatória . . . 114**

3.1 Caveat, *114*; 3.2 Métodos e algoritmos, *115*; 3.3 O problema da complexidade, *120*

**Terminologia de Álgebra Comutativa . . . . 129**

**Bibliografia . . . . . 139**

**Índice remissivo**

CAPÍTULO

**1**

GRAFOS, I: GENERALIDADES

## Capítulo 1 - Grafos, I: Generalidades

**1.1 Grafos como relações.** A teoria dos grafos reveste-se do encanto habitual de todas as teorias que administram um mosaico de aplicações aos vários domínios do conhecimento. Sob pena de desfazer o encanto, usaremos a seguinte formulação abstrata do conceito de grafo.

(1.1.1) DEFINIÇÃO. Um *relgrafo* (resp., um *grafo*) a conjunto de *vértices*  $\mathcal{V}$  é uma relação (resp. uma relação simétrica e não reflexiva) no conjunto  $\mathcal{V}$ .

Suporemos tacitamente, ao longo do texto, que o conjunto  $\mathcal{V}$  é finito.

Do ponto de vista das representações habituais de um grafo, as hipóteses feitas resultam na exclusão de “loops” e na ausência de orientação das arestas. Vários textos referem-se a este caso especial como a de um *grafo simples*, terminologia que evitaremos empregar.

A título de notação, um grafo será indicado por  $G = (\mathcal{V}, \mathcal{A})$ , onde  $\mathcal{V}$  designa o conjunto de vértices e  $\mathcal{A}$ , o subconjunto de  $\mathcal{V} \times \mathcal{V}$  que define  $G$  como relação. Seguindo a tradição da nomenclatura de fundo geométrico, um elemento de  $\mathcal{A}$  é chamado uma *aresta* do grafo.

Sempre que se fizer necessário a consideração simultânea de vários grafos, usaremos as notações  $\mathcal{V}(G)$ ,  $\mathcal{A}(G)$ , etc. Um elemento típico de  $\mathcal{V}$  (resp.  $\mathcal{A}$ ) será denotado por  $v$  (resp.  $a$  ou  $(v_1, v_2)$ ).

Uma formulação alternativa de grafo é obtida decretando-se a existência de dois conjuntos,  $\mathcal{V}$  e  $\mathcal{A}$ , munidos de uma aplicação (chamada *de incidência*)  $\iota : \mathcal{V} \rightarrow \mathcal{A}$ .

Esta definição tem duas vantagens sobre a anterior: primeira, admite a possibilidade de que  $\iota$  seja não injetiva, incluindo *multigrafos* (não serão considerados porque não admitem uma versão algébrica relevante no presente contexto); segunda, entrevê a existência de grafos concretos (isto é, já imersos em espaços familiares – vide 1.2 abaixo).

**1.2 Realização de grafos.** O problema de realização de grafos, à semelhança de outros problemas de realização geométrica, tem fundo nitidamente topológico. Sua formulação depende das aplicações permissíveis para a realização.

Sob risco de pedantismo, propomos, primeiramente, a seguinte noção básica. Um *morfismo* entre dois grafos  $G_1 = (\mathcal{V}_1, \mathcal{A}_1)$  e  $G_2 = (\mathcal{V}_2, \mathcal{A}_2)$  é uma aplicação  $\varphi : \mathcal{V}_1 \rightarrow \mathcal{V}_2$  tal que a aplicação natural induzida

$$\varphi \times \varphi : \mathcal{V}_1 \times \mathcal{V}_1 \rightarrow \mathcal{V}_2 \times \mathcal{V}_2$$

satisfaz a condição adicional  $(\varphi \times \varphi)((v_1, v'_1)) \in \mathcal{A}_2$ , sempre que  $\varphi(v_1) \neq \varphi(v'_1)$ .

Esta última é familiarmente conhecida como a condição de preservação de incidência, pelo seu significado na definição alternativa de grafo dada em 1.1.

Um morfismo é um *isomorfismo* se a aplicação  $\varphi$  é bijetora e a induzida a nível de arestas é sobrejetora (logo, bijetora também). Os grafos são, então, ditos *isomorfos*.

Estritamente, todo grafo isomorfo a um grafo dado é uma realização deste. Estamos mais interessados em realizações de caráter geométrico. Para tal, fazendo uso da segunda definição, consideramos a classe dos grafos obtidos quando impomos aos vértices que sejam pontos do espaço afim  $\mathbb{R}^n$  e que as arestas sejam poligonais ligando um par de vértices, com aplicação de incidência óbvia.

Um tal grafo será dito, um tanto inapropriadamente, *geométrico*. Uma *realização geométrica* de um grafo  $G$  consiste de um grafo  $G'$  geométrico, acompanhado de um isomorfismo  $G \simeq G'$ . Chamamos a atenção do leitor para a confusão habitual entre o isomorfismo e a própria imagem geométrica.

Um grafo geométrico é *imerso* se as arestas se interceptam apenas nos vértices. Um grafo (abstrato) é *geometricamente imersivo* (ou, simplesmente *imersivo*) se for isomorfo a um grafo geométrico imerso.

A terminologia consagrou ainda: um grafo imersivo em  $\mathbb{R}^2$  é dito *planar*. Presumivelmente, a razão pela qual não precisamos nomenclatura para imersividade em espaços de dimensão maior está na seguinte

(1.2.1) PROPOSIÇÃO. *Todo grafo é imersivo em  $\mathbb{R}^3$ .*

DEMONSTRAÇÃO: Seja  $G = (\{v_1, \dots, v_n\}, \{a_1, \dots, a_m\})$  o grafo dado. Tomemos, em  $\mathbb{R}^3$ , duas retas não coplanares transversas  $L_1$  e  $L_2$  e, sobre  $L_1$  (resp.  $L_2$ ) marquemos pontos distintos  $p_1, \dots, p_n$  (resp.  $q_1, \dots, q_m$ ). Introduzamos o grafo geométrico  $\overline{G} = (\overline{\mathcal{V}}, \overline{\mathcal{A}})$  em  $\mathbb{R}^3$  assim definido: primeiramente,  $\overline{\mathcal{V}} = \{p_1, \dots, p_n\}$ ; em seguida, subentendidas as bijeções  $v_i \mapsto p_i$

e  $a_k \mapsto q_k$ , dada uma aresta  $a_k = (v_i, v_j)$  de  $G$ , consideremos a poligonal formada pela sequência dos dois segmentos de reta  $\overline{p_i q_k}$  e  $\overline{q_k, p_j}$ . O conjunto das poligonais assim formadas constitui  $\overline{A}$ .

É imediato que a associação descrita é um isomorfismo entre os dois grafos. ■

Na Figura 1.1, vemos uma ilustração da proposição.

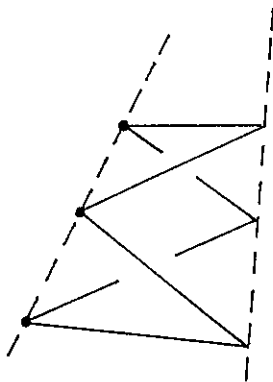


Fig. 1.1 Uma imersão do “triângulo”

(1.2.2) OBSERVAÇÃO. Não há nada especial na escolha dos pontos sobre uma reta. É fácil ver que a figura acima é um nó desatável em  $\mathbb{R}^3$  e que podemos retificar as poligonais a fim de obter a figura usual do triângulo euclidiano, que é planar. Mas, mesmo grafos não planares são passíveis de realizações diferentes em  $\mathbb{R}^3$ , uma para cada gosto. A Figura 1.2 ilustra uma imersão do grafo *completo* a cinco vértices, isto é, do grafo obtido unindo-se, dois a dois, todos os vértices de um conjunto com cinco elementos.

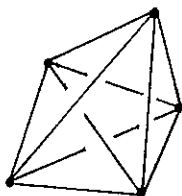


Fig. 1.2 Uma imersão do grafo completo a 5 vértices

A idéia por trás desta realização consiste em, recursivamente, aderir um novo vértice adjacente a todos os vértices do grafo completo de ordem anterior: a partir do triângulo, as arestas de um tetraedro e assim sucessivamente. Intuitivamente, vemos que, procedendo desta maneira, todo grafo completo admite uma realização em  $\mathbb{R}^3$  por arestas que são segmentos de reta, não meramente poligonais – tais realizações são chamadas *retilíneas*.

É importante não confundir uma realização espacial retilínea com uma realização poliédrica (o teorema de Euler para poliedros não nos deixaria!). Temos, na verdade:

- (1) Um poliedro pode ser inscrito numa esfera; conseqüentemente, o conjunto de seus vértices e arestas constituem um grafo planar (pela projeção estereográfica).
- (2) Para um grafo planar  $G = (\mathcal{V}, \mathcal{A})$ , vale a estimativa

$$|\mathcal{A}| \leq 3|\mathcal{V}| - 6.$$

(Em verdade, consequência do teorema de Euler).

- (3) Nem todo grafo admitindo realização retilínea obedece à relação em (2) – por exemplo, o grafo completo a 5 vértices.

Questões desta natureza são típicas da topologia subjacente à teoria dos grafos, algumas delas bastante difíceis e ainda sem solução. Acabamos de observar, por exemplo, que todo grafo poliédrico é planar retilíneo. A recíproca não é verdadeira, como mostra qualquer dos grafos da Figura 1.3.

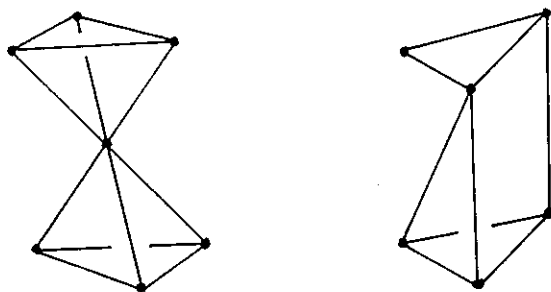


Fig. 1.3 Grafos retilíneos planos não poliédricos

Com a hipótese adicional de que o grafo é *3-conexo* – isto é, de que são necessários ao menos três vértices a fim de que, retirados estes vértices, juntamente com as arestas a eles incidentes, o grafo restante admita ao

menos duas componentes conexas – a recíproca vale e é devida a E. Steinitz [StRa34].

Para realizações poliédricas em dimensão superior a três, não se conhecem condições necessárias e suficientes.

**1.3 Grafos e seus automorfismos.** Um *automorfismo* de um grafo  $G$  é um isomorfismo de  $G$  em  $G$ . O conjunto dos automorfismos de  $G$ , denotado  $Aut(G)$ , admite estrutura de grupo relativamente à composição de aplicações. Fixando uma bijeção de  $\mathcal{V}(G)$  sobre  $\{1, \dots, n\}$ , sendo  $n$  o cardinal de  $\mathcal{V}(G)$ , identificamos  $Aut(G)$  com um subgrupo do grupo de permutações  $S_n$ .

O *grau* (ou *valência*) de um vértice de  $G$  é o número de arestas incidentes neste vértice. Uma das propriedades facilmente reconhecíveis de um automorfismo é de que os graus dos vértices são preservados. Os grafos da Figura 1.4 mostram que uma bijeção de  $\mathcal{V}(G)$ , gozando desta propriedade, não determina necessariamente um automorfismo.

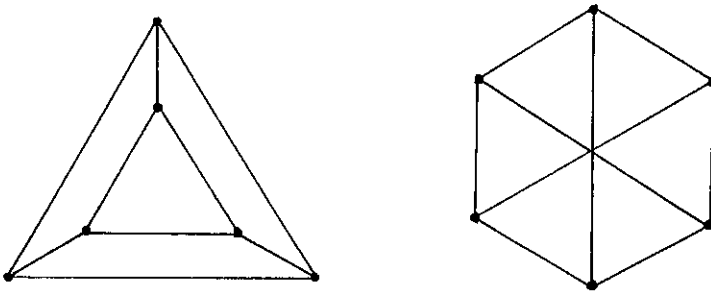


Fig. 1.4 Grafos não isomorfos, com mesma seqüência de graus

Neste caso, é fácil decidir que os dois grafos não são isomorfos; por exemplo, o primeiro admite ciclos ímpares, enquanto o segundo só admite ciclos pares – um grafo *bipartido* (vide 1.5).

Evidentemente, não existe uma maneira óbvia de determinar  $Aut(G)$  em geral. As diversas técnicas de realização de grafos constituem um instrumento útil para determinação de  $Aut(G)$ . Assim, por exemplo, um grafo admitindo realização geométrica com imagem um polígono (não necessariamente convexo) de  $n$  lados, tem grupo de automorfismos isomorfo ao grupo de simetrias deste polígono – o chamado grupo *diédrico*  $D_n$ , de ordem  $2n$ .



(1.3.1) EXEMPLO.  $Aut(K_n) \simeq S_n$ , onde  $K_n$  denota o grafo completo a  $n$  vértices.

O leitor poderá demonstrar esta afirmação, a título de exercício.

Um pouco mais interessante é o seguinte.

(1.3.2) EXERCÍCIO. Seja  $G = (\mathcal{V}, \mathcal{A})$ , onde  $\mathcal{V} = \{v_1, v_2, v_3, v_4\}$  e  $\mathcal{A} = \{(v_1, v_2), (v_3, v_4)\}$ . Pede-se:

- (1) Decidir se  $Aut(G)$  é um grupo abeliano.
- (2) Calcular a ordem de  $Aut(G)$ .
- (3) Determinar a estrutura de  $Aut(G)$ .

Pode-se mostrar que o grupo de automorfismos da união disjunta de  $m$  cópias de um grafo conexo  $G$  é isomorfo ao grupo de permutações em  $m$  símbolos convenientemente composto com  $Aut(G)$  – um grupo de ordem  $m! |Aut(G)|^m$ , bastante grande.

Tendo adquirido certa habilidade com o manuseio destes exemplos, o leitor deverá ser capaz de decidir o próximo.

(1.3.3) EXERCÍCIO. É verdade que dois grafos, cujos respectivos grupos de automorfismos são isomorfos, são isomorfos também? (Pede-se uma demonstração ou um contra-exemplo).

Intuitivamente,  $Aut(G)$  depende das “simetrias” de  $G$ . Em particular, poder-se-ia esperar que a existência de um grande número de vértices do mesmo grau fosse responsável pelo crescimento de  $Aut(G)$ , num sentido a ser precisado.

A natureza, contudo, nos reserva algumas surpresas.

Um grafo é dito *d-regular* se todos seus vértices têm grau  $d$ . Grafos regulares constituem, por assim dizer, o melhor caso-teste para questões sobre isomorfismos e sobre  $Aut(G)$ .

Na próxima seção, veremos como os graus dos vértices intervêm em certas propriedades do grafo relacionadas com a coloração.

Ora bem, R. Frucht [Fru38] demonstrou que todo grupo é isomorfo a  $Aut(G)$  para algum grafo  $G$ . Em particular, existem grafos cujo grupo de automorfismos reduz-se à identidade.

Na Figura 1.5, um grafo 3-regular, com menor número de vértices possível, cujo grupo de automorfismos é trivial.

Frucht nao ceceu os direitos, que pena!

Tente seu proprio exemplo

**Fig. 1.5** O grafo 3-regular de Frucht, sem automorfismos

(1.3.4) EXERCÍCIO. Dar um exemplo de árvore  $T$  com 7 vértices tal que  $\text{Aut}(T) = \{1\}$ . (*Sugestão: 3 vértices terminais são suficientes*)

(1.3.5) EXERCÍCIO. Construir um grafo  $G$  tal que  $\text{Aut}(G) \simeq \mathbb{Z}/3\mathbb{Z}$  (*Atenção: o número de vértices é pelo menos 9*).

O leitor é seriamente estimulado a tentar uma solução, antes de recorrer ao trabalho de Harary e Palmer [HaPa73].

**1.4 Subgrafos e árvores geradoras.** A noção principal deste parágrafo é de substancial aplicação em problemas de complexidade. Neste curso, seu interesse está limitado a certas situações em que a configuração de subgrafos desempenha algum papel.

(1.4.1) DEFINIÇÃO. Um subgrafo  $H$  de um grafo  $G$  é chamado um *subgrafo gerador* (ingles: “spanning”) se  $\mathcal{V}(H) = \mathcal{V}(G)$ .

Uma das principais motivações para destacar este conceito é o problema do ciclo hamiltoniano. Um ciclo de um grafo  $G$  é *hamiltoniano* se for um subgrafo gerador de  $G$  – neste caso, é tradicional chamar o próprio  $G$  de hamiltoniano.

Existem obstruções para um grafo ser hamiltoniano e o leitor poderá se divertir, procurando algumas delas. Em geral, não se conhecem condições não triviais que caracterizem os grafos hamiltonianos e o problema de encontrar um ciclo hamiltoniano (se existir) – a exemplo do problema do caixeiro viajante – faz parte da lista de problemas NP-completos (vide *Palimpsesto 3*).

Um caso particular importante de estrutura geradora é o de uma árvore geradora. Um *conjunto desconector* (ingles: “cutset”) de um grafo  $G$  é um subconjunto  $D \subset \mathcal{A}(G)$  tal que  $\mathcal{A}(G) \setminus D$  tem mais componentes conexas do que  $G$ . Conjuntos desconectores de vértices também fazem sentido e um

problema relacionado com os mesmos foi brevemente mencionado acima, a propósito do teorema de Steinitz–Rademacher (vide 1.3).

Um dos poucos resultados sobre árvores geradoras neste curso, cuja demonstração poderá ser suprida pelo leitor, é o seguinte.

(1.4.2) PROPOSIÇÃO. *Seja  $G$  um grafo conexo (isto é, dois vértices quaisquer estão conectados por um caminho) e seja  $T$  uma árvore geradora de  $G$ . Valem:*

(i) *Para toda aresta  $a \in \mathcal{A}(G) \setminus \mathcal{A}(T)$ ,  $G$  admite um único ciclo contendo  $a$  e arestas de  $T$ ;*

(ii) *Para toda  $a \in \mathcal{A}(T)$ , existe um único conjunto desconector  $D \subset \mathcal{A}(G)$  consistindo de  $a$  e arestas não pertencentes a  $T$ .*

Esta proposição esclarece resultados sobre o *espaço de ciclos* de um grafo  $G$ , tema relacionado com a fórmula de Euler para poliedros. Ambos serão mencionados mais adiante (vide 2.4 e Cap. 4).

Na literatura de árvores geradoras, é familiar a noção de *complexidade* de um grafo, pela qual se entende o número de árvores geradoras de  $G$  – seria mais apropriada a designação *complexidade arbórica*, uma vez que o problema da complexidade em teoria dos grafos tem facetas diversas.

Na teoria das representações matriciais de grafos (leia-se: matrizes de adjacência, de incidência, de circuito, etc.), a complexidade arbórica aparece de modo natural, em conexão com vários resultados clássicos de obtenção da mesma [Cay889], [Tem64], [Moo67].

**1.5 Coloração de vértices e grafos  $r$ -partidos.** O problema de colorir os vértices de um grafo é um dos tópicos mais atraentes e provocativos da teoria.

Seja  $G = (\mathcal{V}, \mathcal{A})$  um grafo; uma *coloração* ou uma *cromatização* (dos vértices) de  $G$  é uma partição de  $\mathcal{V}$  em subconjuntos  $\mathcal{V}_1, \dots, \mathcal{V}_r$  tal que  $\mathcal{A} \cap \bigcup_{i=1}^r (V_i \times V_i) = \emptyset$ . Em outras palavras, vértices adjacentes devem pertencer a subconjuntos distintos da partição.

Em linguagem imprecisa, mas sugestiva, os conjuntos  $V_i$  são chamados *cores*. Dois números são, evidentemente, importantes: o cardinal  $r$  da partição (isto é, o número de cores) e o número  $\pi_G(r)$  de colorações a  $r$  (ou menos) cores. Birkhoff e Lewis foram os primeiros a investigar esta função aritmética associada a grafos e a demonstrar que ela é um polinômio em  $r$  para todos os valores de  $r$  (não apenas assintoticamente, como é típico de outras funções aritméticas – vide 3.1, por exemplo).

O polinômio  $\pi_G(r)$  é conhecido como o *polinômio cromático* de  $G$ ; o menor cardinal possível  $\chi(G)$  de uma coloração de  $G$  é chamado o *número cromático* de  $G$ .

(1.5.1) EXERCÍCIO. (i) Calcule  $\pi_G(r)$  e  $\chi(G)$ , onde  $G = K_n$  (o grafo completo a  $n$  vértices).

(ii) Calcule  $\pi_G(r)$ , onde  $G$  é um grafo bi-cromatizável (isto é,  $\chi(G) \leq 2$ ).

Existem muitos resultados sobre estes dois invariantes. Uma coloração de um grafo  $G = (\mathcal{V}, \mathcal{A})$  será chamada também de *partição* de  $G$ . Existe um tênue risco de confusão com uma partição do conjunto  $\mathcal{V}$ , o que procuraremos evitar. Neste espírito, um grafo  $r$ -cromatizável será chamado  *$r$ -partido*.

## 1.6 Conjuntos parcialmente ordenados.

Neste parágrafo suporemos, como antes, que todos os conjuntos relevantes são finitos. Uma parte substancial das noções que seguem se estendem imediatamente ao caso infinito, mas não faremos uso disto.

Um *conjunto parcialmente ordenado* é um conjunto  $\mathcal{P}$ , munido de uma ordem parcial  $\leq_{\mathcal{P}}$ . Normalmente, a ordem vem subentendida no contexto, de modo que a notação  $\leq$  será suficiente.

Uma *cadeia* de  $\mathcal{P}$  é um subconjunto totalmente ordenado  $\mathcal{C} : a_1 < \dots < a_m$  de  $\mathcal{P}$ . O *posto* de uma cadeia  $\mathcal{C}$ , denotado  $r(\mathcal{C})$ , é o número de elementos da cadeia (incluindo os extremos!); o posto de um conjunto parcialmente ordenado  $\mathcal{P}$ , denotado  $r(\mathcal{P})$ , é o máximo dos postos de suas cadeias. Um conjunto parcialmente ordenado é *catenário* (“ranked”, na terminologia combinatória) se todas as cadeias máximas de  $\mathcal{P}$  têm o mesmo posto.

Um subconjunto  $\mathcal{I} \subset \mathcal{P}$  é um *ideal de ordem* ou, simplesmente, um *ideal*, se sempre que  $a \in \mathcal{I}$  e  $b \in \mathcal{P}$  for tal que  $b \leq a$ , então  $b \in \mathcal{I}$  - revertendo o sinal  $\leq$  na definição, obtemos o conceito de *filtro*. Exemplos importantes de ideais de ordem são os ideais *elementares*  $\mathcal{I}(a) := \{b \in \mathcal{P} \mid b \leq a\}$ , um para cada  $a \in \mathcal{P}$  (o elemento  $a$ , em alguns contextos, é excluído do ideal).

Para questões de representação mais finas, é usada a noção de *multicadeia*. Trata-se de uma cadeia  $\mathcal{C} : a_1 < \dots < a_m$  munida de um vetor de *multiplicidades* ou *pesos*  $p = (p_1, \dots, p_m)$ , um peso para cada elemento  $a_i$  da cadeia. A notação para uma multicadeia, se realmente se fizer necessário, é  $(\mathcal{C}, p)$ ; neste caso, dizemos, por vezes, que a cadeia  $\mathcal{C}$  é o *suporte* da multicadeia  $(\mathcal{C}, p)$ . Finalmente, temos a noção de *multiposto* de uma multicadeia

$(\mathcal{C}, p)$ , denotado  $r(\mathcal{C}, p)$ , que é o vetor

$$(r(a_1), \dots, r(a_m)).$$

Uma multicadeia pode ser convenientemente representada por monômios - mais precisamente, por termos monomiais (vide 3.1). Para tal, primeiramente, fixamos uma ordenação dos elementos do conjunto parcialmente ordenado  $\mathcal{P}$  compatível com a ordem subjacente. Em seguida, estabelecemos uma bijeção ordenada entre  $\mathcal{P}$  e um conjunto de variáveis  $X_1, \dots, X_n$  sobre um corpo  $k$ . Finalmente, dada uma multicadeia de suporte  $\mathcal{C} : a_1 < \dots < a_m$  e vetor de pesos  $p = (p_1, \dots, p_m)$ , o monômio associado é

$$M(\mathcal{C}, p) := X_1^{p_1}, \dots, X_m^{p_m}.$$

No capítulo 3, veremos como estes monômios formam um anel e como as propriedades do conjunto parcialmente ordenado são capturadas nas propriedades algébricas.

(1.6.1) EXEMPLOS. (i) Seja  $V$  um conjunto qualquer. O conjunto  $2^V$  de todos os subconjuntos de  $V$  (em geral, excluimos  $\emptyset$ ) forma um conjunto parcialmente ordenado.

(ii) Numa primeira definição, um *complexo simplicial* baseado no conjunto  $V$  é um ideal de ordem no conjunto parcialmente ordenado  $2^V$  acima. Neste caso, os elementos mínimos do ideal de ordem são chamados *vértices* do complexo simplicial - mais tarde exigiremos (vide 2.4) que os elementos mínimos do complexo sejam da forma  $\{v\}$ , com  $v \in V$ .

(iii) Se  $\mathcal{P}$  é um conjunto parcialmente ordenado, o conjunto dos seus ideais de ordem formam um novo conjunto parcialmente ordenado, com respeito à relação de inclusão de subconjuntos. Este conjunto parcialmente ordenado é chamado de *transformado dos ideais* de  $\mathcal{P}$ . Notação:  $\mathcal{I}(\mathcal{P})$ . Pode-se verificar que este conjunto parcialmente ordenado é um reticulado distributivo e que, em essência, todo reticulado distributivo é desta forma; neste curso, teremos pouco uso para este fato.

(iv) Seja  $\mathcal{P}$  um conjunto parcialmente ordenado catenário de posto  $r$  e seja  $S \subset \{1, \dots, r\}$ . O conjunto parcialmente ordenado dito obtido por *escolha de S-posto*, é o sub-conjunto parcialmente ordenado  $\mathcal{P}_S := \{a \in \mathcal{P} \mid r(\mathcal{I}(a)) \in S\}$ . Este conjunto parcialmente ordenado assim derivado, desempenha algum papel na teoria dos conjuntos parcialmente ordenados de

Cohen–Macaulay (vide 4.1 para a noção básica de estruturas de Cohen–Macaulay).

(1.6.2) DEFINIÇÃO. Seja  $\mathcal{P}$  um conjunto parcialmente ordenado. Dizemos que um elemento  $a \in \mathcal{P}$  cobre um elemento  $b \in \mathcal{P}$  se  $b < a$  e esta cadeia é saturada (no sentido de que não admite inserções próprias). O diagrama de Hasse de  $\mathcal{P}$ , denotado  $\mathcal{H}(\mathcal{P})$ , é o grafo cujo conjunto de vértices é  $\mathcal{P}$  e cujas arestas correspondem a pares  $(a, c)$  tais que  $a$  cobre  $c$ .

O diagrama de Hasse é muito usado na teoria dos reticulados e, mais, particularmente, na teoria dos grupos e corpos. Apesar de ser um grafo (simples) por definição, o diagrama de Hasse é tratado, quase sempre, como um grafo com arestas dirigidas (se  $a$  cobre  $c$ , a aresta é  $\overrightarrow{ca}$ ) ou um grafo munido de posto (“ranked graph”, em inglês).

CAPÍTULO **2**

GRAFOS, II: COMPLEXIDADE

## Capítulo 2. Grafos, II: Complexidade

### COMPLEXIDADE ALGORÍTMICA

#### 2.1 Coberturas de vértices.

Seja  $G = (\mathcal{V}, \mathcal{A})$  um grafo. Uma das noções extensivamente usadas neste curso é a de *cobertura de vértices* de  $G$ . Por esta entende-se um subconjunto  $C \subset \mathcal{V}$  tal que toda aresta de  $G$  é incidente a pelo menos um vértice pertencente a  $C$ .

Trata-se de uma noção simples, mas faz parte da família de problemas NP-completos (vide *Palimpsesto 3*). A idéia intuitiva de procurar vértices de maior grau possível pode não ser sempre a melhor estratégia para determinar uma cobertura de vértices menor possível e, dependendo do problema, pode ser mais interessante começar com vértices de grau pequeno.

(2.1.1) DEFINIÇÃO. O *número de cobertura de vértices* de  $G$  é o cardinal de uma cobertura de vértices com o menor número possível de vértices.

A notação mais ou menos tradicionalmente aceita, para o número de cobertura de vértices é  $\alpha_0(G)$ .

(2.1.2) EXEMPLO. Para qualquer  $n$ , tem-se  $\alpha_0(K_n) = n - 1$ .

(2.1.3) EXERCÍCIO. Para quaisquer valores  $m_1, \dots, m_r$ , tem-se

$$\alpha_0(K_{m_1, \dots, m_r}) = \min_{1 \leq i \leq r} \left\{ \sum_{j \neq i} m_j \right\}.$$

(2.1.4) EXEMPLO. Dê exemplo de um grafo  $G$  bipartido, não completo, admitindo uma partição de tipo  $\{m, n\}$  tal que  $\alpha_0(G) < \min\{m, n\}$ .

Uma das dificuldades da teoria reside no fenômeno de que duas coberturas de vértices mínimas (no sentido de não conterem propriamente qualquer cobertura de vértices) podem ter cardinais diferentes. Introduzimos, por esta razão, um segundo número de cobertura, a saber, o cardinal de uma cobertura mínima de vértices de  $G$  com o maior número possível de vértices, que será denotado  $\alpha_\infty(G)$ . Claramente, temos  $\alpha_0(G) \leq \alpha_\infty(G)$ . No caso de igualdade, dizemos que o grafo é *puro* (ou *não misto*, do ingles “unmixed”). Grafos puros são importantes e serão retomados mais adiante.



A fim de introduzir o próximo número de cobertura, é conveniente usar a seguinte nomenclatura. Dado um subconjunto  $W \subset \mathcal{V}(G)$ , o *conjunto vizinho* ou a *vizinhança* de  $W$ , denotado  $\mathcal{N}_G(W)$ , é o conjunto de todos os vértices de  $G$  adjacentes a algum vértice pertencente a  $W$ . Por convenção, incluímos na vizinhança de  $W$  os vértices a ele pertencentes (mesmo no caso em que os vértices de  $W$  não formem arestas).

A *vizinhança de ordem  $p$*  de  $W$  é definida por recorrência:

$$\mathcal{N}^{[1]}(W) := \mathcal{N}(W); \quad \mathcal{N}^{[p]}(W) := \mathcal{N}(\mathcal{N}^{[p-1]}(W)).$$

Finalmente, o *subgrafo menos  $W$*  é o subgrafo  $G - W$  de  $G$  induzido pelo subconjunto complementar  $\mathcal{V}(G) \setminus \mathcal{N}(W)$  – isto significa que os vértices de  $G - W$  são os elementos de  $\mathcal{V}(G) \setminus \mathcal{N}(W)$  e as arestas, as arestas de  $G$  cujos vértices (ambos) pertencem a este subconjunto.

O terceiro número que reflete um fenômeno de cobertura, localmente, num vértice do grafo  $G$ , é definido da seguinte maneira.

(2.1.5) DEFINIÇÃO. Seja  $v \in \mathcal{V}(G)$ . O *número de cobertura de vértices de primeira ordem em  $v$*  é o número

$$\alpha^{[1]}(v) := \alpha_0(G - \mathcal{N}(v)) + d(v),$$

onde  $d(v)$  denota o grau de  $v$ .

Eis a relação entre os três números descritos:

(2.1.6) PROPOSIÇÃO. *Se  $G$  é um grafo sem vértices isolados, tem-se*

$$\alpha_0(G) \leq \alpha^{[1]}(v) \leq \alpha_0(G) + \alpha_\infty(G)$$

para todo vértice  $v \in \mathcal{V}(G)$ .

DEMONSTRAÇÃO: Para obter a desigualdade da esquerda, procedemos da seguinte forma. Primeiramente, observemos que toda cobertura mínima de  $G$  tem de conter  $v$  ou todos os vértices propriamente adjacentes a  $v$  (possibilidades mutuamente exclusivas). Queremos mostrar que, dada uma cobertura mínima  $C_v$  de  $G - \mathcal{N}(v)$ , existe uma cobertura de  $G$  cujo cardinal não excede  $\#C_v + d(v)$ . Distinguímos dois casos, conforme  $C_v$  contenha ou não algum vértice pertencente a  $\mathcal{N}^{[2]}(v)$ . Deixamos ao leitor, a título de

exercício, a verificação de que, em qualquer dos casos, a desigualdade desejada segue.

Quanto à segunda desigualdade, podemos supor, sem perda de generalidade, que o vértice  $v$  tem grau maior possível entre os vértices de  $G$ . É fácil ver que a desigualdade em questão segue desta outra:  $d(v) \leq \alpha_\infty(G)$ . Para obter esta última, observemos que existe ao menos uma cobertura mínima de vértices, digamos  $C$ , que não contém  $v$  (porque?). Neste caso, todos os vértices adjacentes a  $v$  pertencem a  $C$ , o que nos diz que  $d(v) \leq \#C \leq \alpha_\infty(G)$ , como queríamos. ■

(2.1.7) COROLÁRIO. Se  $G$  é um grafo puro, sem vértices isolados, então vale

$$\alpha_0(G) \leq \alpha^{[1]}(v) \leq 2\alpha_0(G)$$

para todo  $v \in \mathcal{V}(G)$ .

Eis algumas considerações adicionais sobre os números acima.

- (1) A segunda desigualdade em (2.1.7) falha, praticamente por qualquer valor prescrito, se o grafo não é puro, como se verifica facilmente no caso de um grafo bipartido  $K_{1,n}$  (“estrela”) ou de um grafo *roda*  $W_n$ , para  $n \geq 7$  (vide Figura 2.1).
- (2) Muitos grafos bipartidos não puros, de tipo  $\{n, n\}$  – tais como um ciclo par – satisfazem a segunda desigualdade em (2.1.7).
- (3) Por analogia, podemos introduzir números de cobertura de ordem superior,  $\alpha^{[m]}(v)$  ( $m \geq 1$ ), relacionados com os subgrafos  $(G - v)^{[m]}$ . Seria interessante descobrir estimativas para estes números em termos de invariantes numéricos do grafo  $G$ .

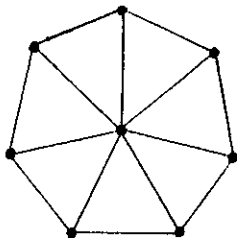


Fig. 2.1 O grafo *roda*

Uma medida da simetria de um grafo é a sua regularidade (vide 1.3). Medida de simetria mais fina é fornecida pela seguinte noção.

(2.1.8) DEFINIÇÃO. Seja  $G$  um grafo. O *vetor de cobertura de primeira ordem* de  $G$  (definido a menos de ordenação dos vértices) é a  $n$ -upla cuja  $i$ -ésima coordenada é o número de cobertura de primeira ordem do vértice  $v_i \in \mathcal{V}(G)$ .

(2.1.9.) EXEMPLOS. (i) O vetor de primeira ordem de  $K_n$  é o vetor diagonal  $(n-1, \dots, n-1)$ .

(ii) Para um grafo bipartido completo  $K_{m,n}$ , o vetor de primeira ordem é

$$\underbrace{(n+m-1, \dots, n+m-1)}_{m \text{ vezes}}, \underbrace{(m+n-1, \dots, m+n-1)}_{n \text{ vezes}}.$$

(ii) O vetor de primeira ordem de um ciclo  $C_n$  é

$$(2 + \lfloor \frac{n-3}{2} \rfloor, \dots, 2 + \lfloor \frac{n-3}{2} \rfloor),$$

onde  $\lfloor q \rfloor$  designa a parte inteira do número racional  $q$ .

(2.1.10) EXERCÍCIO. Uma árvore pode admitir vetor de primeira ordem cujas coordenadas são todas iguais?

Um dos invariantes de um grafo  $G$ , ligado aos números de cobertura, é o número cromático  $\chi(G)$ .

(2.1.11) PROPOSIÇÃO. Para todo grafo  $G$ , tem-se

$$\chi(G) - 1 \leq \Delta(G) \leq \alpha_\infty(G),$$

onde  $\Delta(G)$  denota o máximo dos graus dos vértices de  $G$ .

DEMONSTRAÇÃO: A desigualdade da direita foi obtida no curso da demonstração de (2.1.6). A desigualdade da esquerda é um dos resultados mais simples da teoria do número cromático; deixaremos a demonstração como exercício para o leitor. ■

O grafo roda  $W_n$  põe em evidência que não se pode, a título de melhorar a desigualdade da direita, substituir  $\alpha_\infty(G)$  por  $\alpha_0(G)$ . Contudo, se estivermos dispostos a sacrificar  $\Delta(G)$ , existe o seguinte refinamento.

(2.1.12) PROPOSIÇÃO. Para todo grafo  $G$ , vale  $\chi(G) - 1 \leq \alpha_0(G)$ .

DEMONSTRAÇÃO: Procedemos por indução sobre o número de vértices.

Começamos com um vértice arbitrário  $v$ ; se  $v$  é crítico por cobertura – no sentido de que  $\alpha_0(G - v) < \alpha_0(G)$  – então o resultado é imediato uma vez que  $\chi(G) \leq \chi(G - v) + 1$  sempre vale.

Se  $v$  não é crítico por cobertura, podemos supor que  $v$  seja adjacente a pelo menos um vértice em cada um dos conjuntos  $S_1, \dots, S_r$  da partição associada a uma coloração mínima – pois, se assim não fôra, teríamos  $\chi(G) = \chi(G - v)$ , em cujo caso o resultado procurado seguir-se-ia uma vez mais.

Por outro lado, o complemento de, digamos,  $S_1$ , contém uma cobertura de vértices mínima de  $G - v$ , ao passo que uma cobertura mínima do grafo original  $G$ , conforme foi observado mais acima, deve conter  $v$  ou todos os vértices pertencentes a  $S_1$  e adjacentes a  $v$ . Mas, isto representa uma contradição face à não-criticalidade de  $v$ . ■

**2.2 Conjuntos independentes.** Esta noção, a rigor, dispensaria apresentação, uma vez que é complementar à de cobertura de vértices. Contudo, pelo seu uso intenso e pela sua importância, merece ser mencionada.

(2.2.1) DEFINIÇÃO. Seja  $G$  um grafo. Um subconjunto de  $\mathcal{V}(G)$  é dito *independente* se dois quaisquer de seus vértices são não adjacentes.

Exemplo de conjunto independente é o conjunto unitário formado por um vértice! Se bem que, em alguns casos estes sejam os únicos, em geral estaremos preocupados com outros, contendo mais vértices.

É fácil ver que o complementar de um conjunto independente é uma cobertura de vértices (*Cuidado*: tomar o complementar não significa negar a propriedade que define um conjunto independente). Em particular, o complementar de uma cobertura mínima é um conjunto independente máximo.

Como no caso de coberturas, introduzimos a noção de *número de independência*  $\beta_0(G)$  do grafo  $G$  como sendo a do cardinal maior possível de conjuntos independentes máximos. Desta forma, temos a relação

$$n = \alpha_0(G) + \beta_0(G)$$

onde  $n$  é o número de vértices de  $G$ .

(2.2.2) EXERCÍCIO. Determine, para cada um dos exemplos de grafos mencionados no texto, os conjuntos independentes máximos e o número de independência respectivo.

Considerações análogas podem ser feitas para realçar as arestas, em vez dos vértices, de  $G$ , com a conseqüente definição numerológica. Neste curso, porém, só faremos uso dos números referentes aos vértices (exceto, por suposto, o número total de arestas de  $G$ ).

Finalmente, diremos que existe uma vasta literatura especializada sobre independência – nem sempre, com esta terminologia. No curso, nenhuma estimativa especial ou técnica complicada, oriundas desta literatura, serão utilizadas. O leitor pode passar despreocupado às seções seguintes, mas antes deverá ter um exemplo, através das proposições abaixo, da típica consideração que se faz, no curso, destas noções.

(2.2.3) PROPOSIÇÃO. *Seja  $G$  um grafo conexo tal que  $\chi(G) = 2$ . Então*

- (1)  *$G$  admite uma única bi-coloração, isto é, uma partição unicamente definida  $\mathcal{V}(G) = C_1 \sqcup C_2$  tal que  $C_1$  and  $C_2$  sejam conjuntos independentes.*
- (2) *As cores  $C_1$  and  $C_2$  são coberturas mínimas de  $G$ .*

DEMONSTRAÇÃO: (1) Procederemos por indução sobre o número de vértices de  $G$ , distinguindo dois casos.

(i)  $G$  admite um vértice  $v$  de grau 1.

Neste caso, é claro que o grafo  $G - v$  é ainda (bipartido e) conexo. Pela hipótese indutiva,  $G - v$  admite uma única bi-cromatização  $\{C'_1, C'_2\}$ . Se incluímos  $v$  na cor à qual ele não é adjacente, obtemos uma bi-coloração de  $G$ , que é única.

(i) Todo vértice de  $G$  tem pelo menos grau 2.

Neste caso,  $G$  é composto (isto é, é uma reunião conexa) de ciclos (pares, como se verifica imediatamente) e de árvores de um só ramo cada. Além disso,  $G$  admite pelo menos um ciclo, neste caso. Afirmamos, então, a existência de pelo menos um vértice  $v \in \mathcal{V}(G)$  tal que  $G - v$  é ainda (bipartido, certamente, mas também) conexo.

No presente modelo, chamemos um vértice de uma *base de ramallete* se ele for incidente a uma aresta pertencente a uma das árvores uniramadas ou, se pertencer a mais de um ciclo, então dois quaisquer desses ciclos têm em comum duas ou mais arestas. Ora, acontece que nem todo vértice de

$G$  pode ser uma base de ramalhete, pois isto criaria um modelo infinito de grafo (porque?). Assim, consideramos um vértice  $v$  de  $G$  que não é base de ramalhete, o que produz necessariamente, um vértice não desconector de  $G$ .

Pela hipótese indutiva,  $G - v$  admite uma única bi-coloração  $\{C'_1, C'_2\}$ . Para concluir, observamos que  $v$  não pode ser adjacente a ambas as cores. Para constatar isto, basta mostrar que, qualquer que seja o ciclo contendo  $v$ , os dois vértices deste círculo adjacentes a  $v$  pertencem a uma mesma cor. Mas, isto é evidente já que o ciclo é par.

A bi-coloração de  $G$  é, como antes, obtida incluindo  $v$  na cor à qual não é adjacente.

(2) Resulta da definição de conjunto independente. ■

(2.2.4) OBSERVAÇÃO. Enfatizamos que, embora possa ser obtida de subgrafos diferentes, a bi-coloração de  $G$  é, em última instância, única.

O problema da contagem dos conjuntos independentes é de extrema complexidade computacional (vide *Palimpsesto 3*). Um sub-problema importante é a contagem dos conjuntos independentes máximos (atenção, mais uma vez, para a diferença entre conjuntos independentes máximos e conjuntos independentes de maior cardinal possível). Em casos especiais, este admite soluções elegantes.

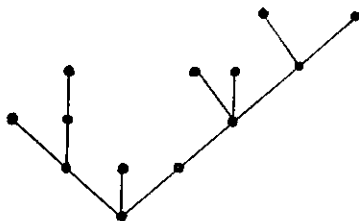
Um dos casos mais manuseáveis é o de árvores. Neste caso, podemos parafrasear a questão em termos de partições, de acordo com a seguinte definição.

(2.2.5) DEFINIÇÃO. Seja  $n > 0$  um número inteiro. Uma *partição ramada* de  $n$  é uma coleção de inteiros positivos  $\{p_i \mid 1 \leq i \leq r\}$  munidos, individualmente, de partição, satisfazendo às seguintes condições:

- (1) A coleção dos  $p_i$ 's forma uma partição de  $n$ ;
- (2)  $p_1 = 1$ ;
- (3) A partição de  $p_i$  tem, quando muito,  $p_{i-1}$  termos, para  $2 \leq i \leq r$ .

A razão destas partições é que elas refletem o comportamento de uma árvore enraizada (daí, exigir  $p_1 = 1$ ), preparada, por assim dizer, para ter um conjunto independente máximo assinalado, por um processo de "exaustão vertical" (vide Figura 2.2).

O caso mais elementar é o das árvores uniramadas.



**Fig. 2.2** Uma árvore enraizada

(2.2.6) PROPOSIÇÃO. Seja  $T$  uma árvore uniramada a  $n$  vértices. Então a partição ramada de  $T$  é a partição trivial  $n = 1 + \dots + 1$  e o número  $\nu_n := \nu(T)$  de conjuntos independentes máximos é obtido através da sequência de Fibonacci defasada:

$$\begin{aligned} \nu_n &= \nu_{n-2} + \nu_{n-1} \\ \nu_1 &= 1, \quad \nu_2 = 2, \quad \nu_3 = 2. \end{aligned}$$

DEMONSTRAÇÃO: A afirmação sobre a partição ramada é evidente. Para calcular  $\nu_n$ , dividimos a coleção de conjuntos independentes máximos em duas classes: os que contêm o vértice correspondente ao tópo da árvore enraizada e os que não contêm este vértice. Com esta tática, não é complicado enxergar a formação fibonacciana. Os detalhes serão deixados como exercício. ■

Uma aplicação interessante deste resultado refere-se a ciclos.

(2.2.7) PROPOSIÇÃO. O número  $\gamma_n := \gamma(C_n)$  de conjuntos independentes máximos de um ciclo  $C_n$  é dado, recursivamente, pela sequência de Fibonacci defasada

$$\begin{aligned} \gamma_n &= \gamma_{n-2} + \gamma_{n-1} \\ \gamma_1 &= 0, \quad \gamma_2 = 2, \quad \gamma_3 = 3. \end{aligned}$$

DEMONSTRAÇÃO: Removemos um vértice  $v$  do ciclo  $C_n$ . É evidente que  $T_{n-1} := C_n - v$  é uma árvore uniramada e que  $\gamma(C_n) = \nu(T_{n-1}) + \gamma(v)$ , onde  $\gamma(v)$  designa o número de conjuntos independentes máximos de  $C_n$  que contêm  $v$ . Ora,  $\gamma(v)$  coincide, como pode ver o leitor, com o número de

conjuntos independentes máximos da árvore uniramada  $T_{n-3} := C_n - \mathcal{N}(v)$ , onde a vizinhança  $\mathcal{N}(v)$  consiste de  $v$  e dos dois vértices a ele adjacentes no ciclo.

Resulta, então

$$\begin{aligned}\gamma_n &= \gamma(C_n) = \nu(T_{n-1}) + \nu(T_{n-3}) \\ &= \nu_{n-1} + \nu_{n-3}.\end{aligned}$$

A conclusão é, agora, imediata. ■

(2.2.8) OBSERVAÇÃO. Em geral, se  $F_n$  designa a sucessão (usual) de Fibonacci, a valores iniciais  $F_0 = F_1 = 1$ , mostra-se que o número de conjuntos independentes máximos de qualquer grafo a  $n$  vértices é limitado por  $F_n$ . A demonstração deste fato pode ser encontrada em [SiVaVi91].

(2.2.9) EXERCÍCIO. Seja  $T$  uma árvore enraizada, com 3 níveis de ramagem (já incluindo a raiz). Deduza uma fórmula para o número de conjuntos independentes máximos de  $T$  (*Sugestão*: se a partição ramada é  $\{p_1 = 1, p_2, p_3 = p_2 - q_2\}$ , onde  $q_2 \geq 0$ , considere, separadamente, os casos  $q_2 = 0$  e  $q_2 > 0$ .)

## COMPLEXIDADE SIMPLICIAL

**2.3 Complexos simpliciais abstratos.** Já vimos o que se entende por um complexo simplicial baseado em, ou a conjunto de vértices,  $V$  (vide 1.6.1).

Doravante, suporemos, tacitamente, que os conjuntos unitários constituídos pelos elementos de  $V$ , pertencem ao complexo. Repetimos a definição, com este adendo.

(2.3.1) DEFINIÇÃO. Um *complexo simplicial abstrato* baseado em, ou a conjunto de vértices,  $V$  é um conjunto  $\Delta$  de subconjuntos de  $V$  satisfazendo as condições seguintes:

( $\Delta_1$ ) Se  $F \in \Delta$  e  $F' \subset F$ , então  $F' \in \Delta$ .

( $\Delta_2$ ) Para todo  $v \in V$ ,  $\{v\} \in \Delta$ .

Os subconjuntos de  $V$ , pertencentes a  $\Delta$ , chamam-se *faces*. A *dimensão* de uma face é o seu cardinal diminuído de uma unidade. A *dimensão* de  $\Delta$  é o máximo das dimensões de suas faces. Uma face é *máxima* se não está propriamente contida em qualquer face de  $\Delta$ .





**Fig. 2.3** Um complexo, o elo e a estrela de um vértice

Existem vários outros complexos que se deduzem de um complexo  $\Delta$ . Para um inteiro  $r$  ( $1 \leq r \leq d$ ), o  $r$ -esqueleto  $\Delta(r)$  de  $\Delta$  é o (sub-) complexo simplicial cujas faces têm dimensão  $\leq r$ .

(2.3.2) OBSERVAÇÃO. Em homotopia, mostra-se que o grupo fundamental de uma realização geométrica de  $\Delta$  depende apenas do esqueleto  $\Delta(1)$ ; daí, a importância deste sub-complexo naquela teoria. Neste curso, a relevância de  $\Delta(1)$  advém do fato de que admite uma estrutura de grafo, cujos vértices são os vértices de  $\Delta$  e cujas arestas correspondem às faces de dimensão 1 do complexo.

Além do 1-esqueleto, outras construções têm relêvo do ponto de vista homológico.

(2.3.3) DEFINIÇÃO. Seja  $\Delta$  um complexo simplicial e  $F \in \Delta$ , uma face. O *elo* de  $F$  em  $\Delta$  é o conjunto

$$el_{\Delta} F := \{E \in \Delta \mid F \cap E = \emptyset, F \cup E \in \Delta\}.$$

A *estrela* de  $F$  (em  $\Delta$ ) é o conjunto

$$est_{\Delta} F := \{E \in \Delta \mid F \subseteq E\}.$$

Evidentemente, o elo de uma face é ainda um complexo simplicial. A estrela não é um complexo simplicial. As duas noções são, a grosso modo, complementares. Numa realização geométrica, a estrela de  $F$  em  $\Delta$  é uma espécie de “vizinhança” de  $F$  no espaço topológico correspondente a  $\Delta$ , admitindo fronteira no sentido de topologia. Estas e outras considerações fazem parte de um primeiro curso de topologia simplicial, escapando aos objetivos deste curso.

A título de ilustração, a Figura 2.3 mostra realizações geométricas destas noções.

Em seguida, passamos a uma noção parentética a de coloração de grafos.

(2.3.4) DEFINIÇÃO. Uma *rotulação* (ingles: “labeling”) de um complexo simplicial  $\Delta$  baseado em  $V$  é uma partição  $\pi = \{V_1, \dots, V_r\}$  de  $V$ , onde  $V_i$  é chamado o *rótulo*  $i$  e um vértice  $v \in V_i$  é  *$i$ -rotulado*. Uma rotulação  $\pi = \{V_i\}$  de  $\Delta$  é equilibrada se, para toda face  $F \in \Delta$ , tem-se  $\# F \cap V_i = 1$  para todo  $i$ . Finalmente, dizemos que  $\Delta$  é *equilibrado* se admite alguma rotulação equilibrada.

(2.3.5) EXEMPLOS. (i) O complexo simplicial de todos os subconjuntos de um conjunto  $V = \{v_1, \dots, v_r\}$  é equilibrado mediante a rotulação unitária  $V = \{v_1\} \sqcup \dots \sqcup \{v_r\}$  (na verdade, a existência de rotulação unitária caracteriza tais complexos).

(ii) Um complexo simplicial que admite como realização um pentágono, não admite rotulação equilibrada.

Complexos equilibrados estão relacionados com outros, chamados puros – o análogo de conjuntos parcialmente ordenados catenários para complexos simpliciais. Um complexo simplicial é *puro* se todas suas faces máximas têm a mesma dimensão.

(2.3.6) PROPOSIÇÃO. Se  $\Delta$  é um complexo simplicial equilibrado, munido de rotulação de cardinal  $r$ , então  $\Delta$  é puro e sua dimensão é  $r$ .

DEMONSTRAÇÃO: Exercício. ■

A recíproca de (2.3.6) não é verdadeira, como bem mostra o exemplo (2.3.5)(ii).

**2.4 Polítopos e  $f$ -vetores.** Este tema é, a rigor, dispensável para a compreensão do curso. A sua inclusão visa dar uma idéia de como problemas semelhantes na área de geometria convexa podem ser tratados por métodos combinatórios.

Chamamos atenção para muitas das afirmações feitas neste parágrafo, que parecem plausíveis, mas cuja justificativa detalhada requer um curso preliminar sobre polítopos (nos moldes de [Grü67] ou [Brø83], por exemplo).

(2.4.1) DEFINIÇÃO. Um *polítopo* é a envoltória convexa de um conjunto finito de pontos num espaço euclidiano.

Lembremos que a envoltória convexa de um conjunto  $V \subset \mathbb{R}^n$  é a interseção de todos os subconjuntos convexos de  $\mathbb{R}^n$  contendo  $V$ . Um politopo é, por conseguinte, uma interseção limitada de semi-espacos fechados de  $\mathbb{R}^n$ . A envoltória afim de  $V \subset \mathbb{R}^n$  é definida de maneira análoga, como sendo a interseção de todos os subespacos afins de  $\mathbb{R}^n$  contendo  $V$ .

A *dimensão* de um politopo é a dimensão de sua envoltória afim. Um politopo de dimensão  $d$  será, frequentemente, chamado de  $d$ -politopo. Uma *face* do politopo  $\mathfrak{P}$  é a interseção  $H \cap \mathfrak{P}$ , para algum hiperplano  $H \subset \mathbb{R}^n$  tal que  $\mathfrak{P}$  está contido em um dos subespacos determinados por  $H$ . É imediato que uma face de um politopo é, por sua vez, um politopo. A terminologia oriunda dos complexos simpliciais será usada livremente para politopos (assim, temos os vértices, as facetas, etc.).

Exemplos importantes de politopos são os simplexos. Lembremos que um conjunto  $V = \{v_0, \dots, v_r\}$  é dito ser independente se, fixado  $v_0$  (a definição independe, *a fortiori*, desta escolha), os elementos  $v_1 - v_0, \dots, v_r - v_0$  do espaco vetorial com origem em  $v_0$  são linearmente independentes. Um  $r$ -simplexo é a envoltória convexa de um conjunto independente de  $r + 1$  pontos num espaco  $\mathbb{R}^n$ .

Um complexo simplicial abstrato admite muitas realizações politópicas em espacos euclidianos, de tal maneira que as faces do complexo se identifiquem com simplexos. Examinemos a noção de realização de complexos simpliciais, de resto análoga a de grafos, considerada em 1.2.

Um *homomorfismo (simplicial)* do complexo simplicial  $\Delta$  no complexo simplicial  $\Delta'$ , baseados em  $V$  e  $V'$ , respectivamente, é uma aplicação  $\delta : V \rightarrow V'$  tal que  $\delta(F)$  é uma face de  $\Delta'$ , para toda face  $F \in \Delta$ .

Chamamos a atenção para a eventualidade de  $\delta$  não ser injetora, podendo ter lugar colapso de vértices. Se  $\delta$  acima fôr bijetora, diremos que induz um *isomorfismo (simplicial)* entre  $\Delta$  e  $\Delta'$ .

(2.4.2) EXERCÍCIO. (i) Determine todos os homomorfismos simpliciais do complexo simplicial de todos os subconjuntos de um conjunto com três elementos. Quais destes são isomorfismos?

(ii) Mostre, por meio de exemplos, que uma bijeção entre os conjuntos respectivos dos vértices de dois complexos simpliciais, não induz automaticamente um isomorfismo entre os complexos.

Finalmente, temos a generalização politópica de um complexo simplicial.

Um *complexo poliédrico* é uma coleção  $\mathcal{D}$  de politopos em  $\mathbb{R}^n$  tal que:

( $\mathcal{D}_1$ ) Se  $\mathfrak{P} \in \mathcal{D}$  e se  $F$  é uma face de  $\mathfrak{P}$ , então  $F \in \mathcal{D}$ ;

( $\mathcal{D}_2$ ) Se  $\mathfrak{P}_1, \mathfrak{P}_2 \in \mathcal{D}$ , então  $\mathfrak{P}_1 \cap \mathfrak{P}_2$  é uma face comum a ambos os politopos.

Um complexo poliédrico é dito ser *simplicial* se seus politopos são simplexos.

Estamos, agora, em condições de definir realizações poliédricas.

(2.4.3) DEFINIÇÃO. Uma *realização poliédrica simplicial* de um complexo simplicial abstrato  $\Delta$  é um isomorfismo simplicial de  $\Delta$  sobre um complexo poliédrico simplicial (em algum espaço euclidiano).

(2.4.4) EXERCÍCIO. Seja  $\Delta$  um complexo simplicial abstrato baseado em  $V = \{v_1, \dots, v_r\}$ ,  $e_i$  o  $i$ -ésimo vetor unitário coordenado de  $\mathbb{R}^n$ . Mostre que a bijeção  $\delta : v_i \mapsto e_i$  induz um isomorfismo de  $\Delta$  sobre o complexo poliédrico simplicial de  $\mathbb{R}^n$  cujos simplexos são as envoltórias convexas dos conjuntos  $\delta(F)$ , com  $F \in \Delta$ .

O procedimento acima realiza, de maneira uniforme, todo complexo simplicial abstrato a  $n$  vértices no  $\mathbb{R}^n$ . Para muitos efeitos, estas realizações não são as mais econômicas.

Muitas realizações usam o modelo que ora passamos a descrever e que, por outro lado, desempenha um papel fundamental na história dos politopos.

(2.4.5) DEFINIÇÃO. Fixemos dois inteiros  $n > d \geq 1$ . Consideremos, em  $\mathbb{R}^d$ , a curva *momento* definida pelas equações paramétricas  $x(t) = (t, t^2, \dots, t^d)$ . Dada uma sequência de números reais  $\underline{t} : t_1 < \dots < t_n$ , o *politopo cíclico de ordem  $n$  (baseado em  $x(\underline{t})$ )* é a envoltória convexa do conjunto  $\{x(t_1), \dots, x(t_n)\}$ . Notação:  $C_{\underline{t}}(n, d)$ .

Trata-se, como se pode verificar, de um politopo (não somente um complexo poliédrico) simplicial: todas suas facetas e, conseqüentemente, faces, são simplexos.

(2.4.6) OBSERVAÇÃO. É possível mostrar que duas sequências  $\underline{t}$  e  $\underline{s}$  de números reais induzem politopos cíclicos *combinatoriamente equivalentes* – noção que pode ser definida rigorosamente. Os complexos induzidos admitem os mesmos invariantes combinatórios, em particular, os mesmos  $f$ -vetores, no sentido que ora descreveremos.

(2.4.7) DEFINIÇÃO. O  $f$ -vetor de um  $d$ -politopo  $\mathfrak{P}$  é a  $(d+1)$ -upla

$$f(\mathfrak{P}) := (f_{-1}(\mathfrak{P}), f_0(\mathfrak{P}), \dots, f_{d-1}(\mathfrak{P})),$$

onde  $f_i(\mathfrak{P})$  denota o número de faces de dimensão  $i$  em  $\mathfrak{P}$  (com a convenção de que  $f_{-1} = 1$ ).

(2.4.8) EXERCÍCIO. Se  $\mathfrak{P}$  é um  $r$ -simplexo, mostre que

$$f_i(\mathfrak{P}) = \binom{i+r+2}{i+1}.$$

Uma das propriedades fundamentais dos politopos cíclicos é assim expressa.

(2.4.9) PROPOSIÇÃO. Para  $1 \leq k \leq \lfloor \frac{d}{2} \rfloor$ , tem-se

$$f_{k-1}(C(n, d)) = \binom{n}{k}.$$

Para uma demonstração deste fato, vide [Brø83]. Em particular, resulta que, para  $d \geq 4$ , existem  $d$ -politopos com um número arbitrariamente prescrito de vértices com a propriedade de que dois vértices quaisquer são adjacentes (isto é, o segmento que os liga é uma face do politopo). Este fenômeno está relacionado com a célebre conjectura da cota superior (vide 4.3).

O problema central da teoria numérico-combinatória dos politopos assim se enuncia.

(2.4.10) PROBLEMA. Descrever a estrutura do conjunto

$$\mathfrak{F}_d := \{ f(\mathfrak{P}) \in \mathbb{Q}^{d+1} \mid \mathfrak{P} \text{ é } d\text{-politopo} \}.$$

Enfatizemos que, embora os  $d$ -politopos possam estar imersos em espaços euclidianos de dimensão arbitrária, os  $f$ -vetores correspondentes pertencem a um espaço de dimensão (fixa)  $d + 1$ . A descrição que se procura é em termos de equações e inequações, preferivelmente polinomiais, mas de outro modo de grau arbitrário.

(2.4.11) DEFINIÇÃO. O hiperplano de  $\mathbb{Q}^d$ , definido pela equação

$$\sum_{i=0}^{d-1} (-1)^i x_i = 1 - (-1)^d$$

é chamado *d-hiperplano de Euler*. Notação:  $\mathcal{E}_d$ .

Um dos poucos resultados gerais para  $\mathfrak{F}_d$  é o seguinte.

(2.4.12) PROPOSIÇÃO.  $\mathfrak{F}_d \subset \mathcal{E}_d \cap \{x_{-1} = 1\} (\subset \mathbb{Q}^{d+1})$ .

A prova deste resultado afasta-se dos objetivos do curso. O leitor curioso poderá recorrer à bibliografia [Brø83]. Não podemos deixar de chamar a atenção para o caso  $d = 2$ , demonstrado em muitos textos elementares.

Se nos restringirmos aos politopos simpliciais, a situação é bem menos afiltiva. Na verdade, para estes, existe uma teoria razoavelmente completa.

Por conveniência, introduzamos a notação

$$\mathfrak{FS}_d := \{ f(\mathfrak{P}) \in \mathbb{Q}^{d+1} \mid \mathfrak{P} \text{ é } d\text{-politopo simplicial} \}.$$

Obviamente,  $\mathfrak{FS}_d \subset \mathfrak{F}_d$ .

(2.4.13) DEFINIÇÃO. O  $d$ -subespaço de Dehn-Sommerville, denotado  $\mathcal{DS}_d$ , é o subespaço de  $\mathbb{Q}^{d+1}$  definido pelas equações

$$x_k - \sum_{j=k}^{d-1} (-1)^{d-1-j} \binom{j+1}{k+1} x_j = 0, \quad -1 \leq k \leq d-2.$$

(2.4.14) OBSERVAÇÃO. Vale sempre a inclusão  $\mathcal{DS}_d \subset \mathcal{E}_d$ , o que se vê fazendo  $k = -1$  nas equações de Dehn-Sommerville.

A parte referente às equações satisfeitas por  $\mathfrak{FS}_d$  é resolvida pelo seguinte resultado.

(2.4.15) TEOREMA. (Dehn, 1905; Sommerville, 1927; Klee, 1963) *Vale a inclusão*

$$\mathfrak{FS}_d \subset \mathcal{DS}_d.$$

DEMONSTRAÇÃO: Seja  $\mathfrak{P}$  um  $d$ -politopo. Dada uma  $k$ -face  $F$  de  $\mathfrak{P}$ , designemos por  $\mathfrak{P}_F$  o politopo cujo reticulado de faces é o *intervalo* de  $F$  a  $\mathfrak{P}$ , definido como o conjunto de todas as faces  $E$  de  $\mathfrak{P}$  tais que  $F \subseteq E \subseteq \mathfrak{P}$ . Pela fórmula de Euler vista acima, aplicada ao politopo  $\mathfrak{P}_F$ , obtemos

$$1 = \sum_{i=-1}^{d-k-2} (-1)^{d-k-1} f_i(\mathfrak{P}_F).$$

Somando para todas as  $k$ -faces de  $\mathfrak{P}$ , obtemos

$$(2.4-1) \quad f_k(\mathfrak{P}) = \sum_{i=-1}^{d-k-2} (-1)^{d-k-1} \sum_{\dim F=k} f_i(\mathfrak{P}_F).$$

Observando que as  $i$ -faces de  $\mathfrak{P}_F$  correspondem a  $(k + i - 1)$ -faces de  $\mathfrak{P}$ , obtemos que o número

$$\sum_{\dim F=k} f_i(\mathfrak{P}_F)$$

é igual ao número de pares  $(E, G)$  tais que  $E \subset G$ , onde  $E$  (resp.  $G$ ) denota uma  $k$ -face (resp. uma  $(k + i - 1)$ -face) de  $\mathfrak{P}$ . Pela mesma razão, este número coincide com

$$\sum_{\dim G=k+i-1} f_k(G).$$

A esta altura usamos a hipótese de que  $\mathfrak{P}$  é simplicial e que, por conseguinte, suas faces são simplexos. Lançando mão de (2.4.8) e substituindo em (2.4-1), chegamos à conclusão desejada. ■

(2.4.16) PROPOSIÇÃO. (i)  $\dim_{\mathbb{Q}} \mathcal{DS}_d \leq \lfloor \frac{d+1}{2} \rfloor$ .

(ii) A envoltória afim de  $\mathfrak{FS}_d$  tem dimensão  $\lfloor \frac{d}{2} \rfloor$ .

Infelizmente, a demonstração nos levaria muito além do plano do curso (vide [Brø83]). Voltaremos, contudo, a questões envolvendo  $f$ -vetores para o caso de complexos simpliciais abstratos (vide 3.7 e 4.3).

(2.4.17) EXERCÍCIO. Verifique o item (i) de (2.4.16) para os casos em que  $d \leq 4$ .

**2.5 Transferências combinatórias.** Por uma *transferência combinatória* entenderemos um ou mais processos de passagem de uma estrutura combinatória a outra – similar ou aparentada – na procura de informações mais profundas sobre os invariantes da estrutura original.

No decorrer do curso, estas transferências ficarão claras, sem que sejamos levados a dar uma definição geral (aliás, inútil).

### Grafo-aresta.

Seja  $G = (\mathcal{V}, \mathcal{A})$  um grafo. O *grafo-aresta* associado a  $G$  é o grafo  $G_a = (\mathcal{U}, \mathcal{B})$ , onde  $\mathcal{U} := \mathcal{A}$  e

$$\mathcal{B} := \{(a_1, a_2) = ((v_{11}, v_{12}), (v_{21}, v_{22})) \in \mathcal{A} \times \mathcal{A} \mid \{v_{11}, v_{12}\} \cap \{v_{21}, v_{22}\} \neq \emptyset\}.$$

(2.5.1) EXERCÍCIO. (i) Mostre que o grafo-aresta de um  $C_n$  é um  $C_n$ .

(ii) Descreva o grafo-aresta associado a um triângulo aumentado com três

arestas livres, uma de cada vértice do triângulo (esta construção chama-se *suspensão* e será considerada com detalhe em 4.5)

(iii) Mostre uma realização plana do grafo-aresta associado a  $K_{3,3}$ , com razoável simetria geométrica (*Sugestão*: considere o modelo hexagonal de  $K_{3,3}$ ).

(2.5.2) EXERCÍCIO. Exibir os grafos-aresta associados a cada um dos grafos da Figura 2.4.

(2.5.3) EXERCÍCIO. (i) Verifique se o número de independência de um grafo e do seu grafo-aresta coincidem.

(ii) Dê exemplos de grafos não isomorfos, admitindo grafos-aresta isomorfos.

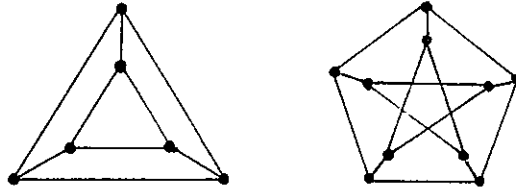


Fig. 2.4 O prisma triangular e o grafo de Petersen

**Grafo complementar.**

O *grafo complementar* de um grafo  $G = (\mathcal{V}, \mathcal{A})$  é o grafo  $G^\perp := (\mathcal{V}, (\mathcal{V} \times \mathcal{V}) \setminus \mathcal{A})$ .

O principal, senão único, interesse desta noção, neste curso, é a relação que guarda com o exemplo seguinte de transferência combinatória.

**Complexos simpliciais oriundos de grafos.**

O conjunto dos subconjuntos de vértices independentes de um grafo  $G$  satisfaz os axiomas de um complexo simplicial abstrato. Em particular, cada vértice, individualmente, é um subconjunto independente de  $G$ ; resulta que  $G$  e o complexo assim construído admitem o mesmo conjunto subjacente de vértices.

Apesar de se tratar de uma importante transferência combinatória, não tem merecido designação especial na literatura (mas, vide [Vil90]). Sempre que necessário, usaremos a terminologia *complexo simplicial grafal* para indicar uma tal construção e a notação  $\Delta(G)$ , para enfatizar o grafo  $G$  que lhe deu origem.



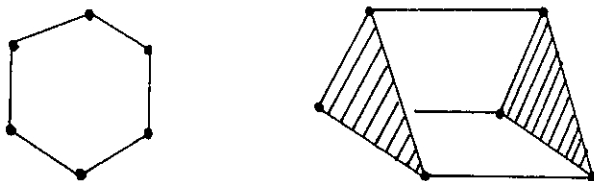


Fig. 2.5 O hexágono e uma realização do complexo associado

A Figura 2.5 mostra uma realização politópica do complexo grafal associado ao hexágono. O leitor poderá considerar realizações dos complexos grafais associados aos diversos grafos já considerados.

Vale o seguinte resultado, cuja verificação é imediata.

(2.5.5) PROPOSIÇÃO. *Seja  $G$  um grafo a conjunto  $V$  de vértices e  $\Delta(G)$  o complexo grafal associado. Então:*

- (1) *A dimensão de  $\Delta(G)$  é igual ao número de independência de  $G$ .*
- (2) *Se  $U \subset V$  não é uma face de  $\Delta(G)$ ,  $U$  contém alguma aresta de  $G$ .*

A segunda afirmação é apenas a definição de conjunto independente, mas será conveniente tê-la sob esta forma.

Como todo complexo simplicial,  $\Delta(G)$  tem uma estrutura subjacente de conjunto parcialmente ordenado. O conjunto parcialmente ordenado obtido, por reversão da relação de ordem, é o conjunto parcialmente ordenado das coberturas de vértices de  $G$ , que será denotado  $\mathcal{C}(G)$ .

$\mathcal{C}(G)$  é mais interessante do ponto de vista algébrico, uma vez que é equivalente (isto é, ordenadamente isomorfo) ao conjunto parcialmente ordenado dos ideais primos contendo o ideal de arestas de  $G$  e gerados por variáveis (vide 3.6). Observemos que  $\mathcal{C}(G)$  (resp.  $\Delta(G)$ ) admite elemento máximo  $\mathcal{V}(G)$  (resp. mínimo  $\emptyset$ ).

Uma transferência combinatória interessante é

$$G \rightsquigarrow \mathcal{H}(\mathcal{C}(G)),$$

onde  $\mathcal{H}(\mathcal{P})$  denota o diagrama de Hasse do conjunto parcialmente ordenado  $\mathcal{P}$  (vide (1.6.2)).

(2.5.6) EXERCÍCIO. Construa o diagrama de Hasse  $\mathcal{H}(\mathcal{C}(G))$  nos seguintes casos:

- (i)  $G = C_n$ , para  $n = 4, 6$ .

- (ii)  $G = C_5$ .  
 (iii)  $G = K_{33}$ .

(2.5.7) EXERCÍCIO. Caracterize os grafos  $G$  para os quais  $\mathcal{H}(\mathcal{C}(G))$  é uma árvore.

(2.5.8) EXERCÍCIO. Seja  $G$  um grafo bipartido (não necessariamente completo). Mostre, por meio de exemplos, que a omissão do elemento máximo de  $\mathcal{H}(\mathcal{C}(G))$  pode ou não desconectar o diagrama.

O problema da “recuperação” de uma estrutura combinatória é comum a todas as transferências. Mesmo assim, gostaríamos de destacá-la no caso especial em consideração.

(2.5.9) PROBLEMA. Qual a relação entre dois grafos  $G_1$  e  $G_2$  cujos Hasianos  $\mathcal{H}(\mathcal{C}(G_1))$  e  $\mathcal{H}(\mathcal{C}(G_2))$  são isomorfos como grafos com posto?

Observe-mos que a transferência

$$G \rightsquigarrow \mathcal{H}(\mathcal{C}(G))$$

é menos fina do que

$$G \rightsquigarrow \mathcal{C}(G),$$

mas, provavelmente, mais fina do que

$$G \rightsquigarrow G_a.$$

### Complexo de cadeias.

(2.5.10) DEFINIÇÃO. Seja  $\mathcal{P}$  um conjunto parcialmente ordenado. O *complexo das cadeias* (ou *complexo de ordem*) associado é o complexo simplicial cujas faces são os subconjuntos de  $\mathcal{P}$  ( $\emptyset$  não incluído) que formam cadeias (vide 1.6) (*Notação:  $\Delta_c(\mathcal{P})$* ).

Observemos que os elementos de  $\mathcal{P}$  são exatamente as cadeias mínimas de  $\mathcal{P}$ , logo os vértices de  $\Delta_c(\mathcal{P})$  coincidem com os elementos do conjunto parcialmente ordenado.

Uma confusão aparente ocorre quando o  $\mathcal{P}$  é o conjunto parcialmente ordenado subjacente a um complexo simplicial abstrato  $\Delta$ . Não há mal essencial em denotar o complexo de ordem associado por  $\Delta_c(\Delta)$ , mas é importante discernir entre este e o complexo simplicial original  $\Delta$ . Precisamente, tem-se:

(2.5.11) PROPOSIÇÃO. *Seja  $\mathfrak{P}$  um politopo. Então  $\Delta(\mathfrak{P})$  tem a estrutura de politopo e, como tal, identifica-se com a divisão baricêntrica completa de  $\mathfrak{P}$ .*

Remetemos o leitor a [EwSh74], para uma demonstração deste resultado.

Julgamento superficial pode induzir a crer que os complexos de cadeias são tão gerais quanto os complexos simpliciais. A um segundo exame, contudo, observamos que existem obstruções *a priori*. Por exemplo, se o complexo admitir um pentágono – isto é, 5 cadeias de dois elementos cada, formando as arestas de um pentágono no 1-esqueleto – então ao menos uma corda do pentágono é uma aresta do 1-esqueleto.

Estas obstruções foram determinadas por Stanley, que caracterizou completamente os complexos de cadeias.

(2.5.12) PROPOSIÇÃO. ([Sta79]) *Seja  $\Delta$  um complexo simplicial. Então  $\Delta$  é um complexo de cadeias (isto é, o conjunto dos vértices de  $\Delta$  admite uma estrutura de conjunto parcialmente ordenado  $\mathcal{P}$  tal que  $\Delta = \Delta_c(\mathcal{P})$ ) se e só se as seguintes condições são satisfeitas:*

- (i)  $\Delta$  é grafal (digamos,  $\Delta = \Delta(G)$ );
- (ii) Todo ciclo de ordem ímpar do grafo complementar  $G^\perp$  admite alguma corda.

Observemos que, conforme visto mais acima, o grafo  $G$  fica completamente determinado, a menos de isomorfismo. Contudo, é concebível que o conjunto de vértices de  $G$  (ou de  $\Delta$ , que é o mesmo) admita várias estruturas de conjunto parcialmente ordenado que dêem origem ao mesmo complexo de cadeias. Novamente, nada se diz sobre o problema da recuperação na transferência combinatória

$$\mathcal{P} \rightsquigarrow \Delta_c(\mathcal{P}).$$

Por outro lado, isto põe em relêvo também o fato de que o conjunto dos vértices de um grafo não admite estrutura natural de conjunto parcialmente ordenado, a não ser passando, intermediariamente, por uma das transferências combinatórias

$$G \rightsquigarrow \Delta(G) \quad \text{ou} \quad G \rightsquigarrow \mathcal{P}(G).$$

Observemos que grafos gozando da propriedade *córdica* mencionada em (ii) admitem um comportamento muito especial em termos das chamadas

“potências simbólicas” do ideal de arestas correspondente (vide *Palimpsesto 2*).

### Comentário

O capítulo de transferências combinatórias não termina aqui. Existem inúmeras variações em torno do tema, algumas completamente desconhecidas por este autor, outras menos interessantes. Por exemplo, um grafo pode ser transferido a um conjunto parcialmente ordenado, simplesmente decretando-se que os elementos do conjunto subjacente ao conjunto parcialmente ordenado são os vértices do grafo e que dois elementos são comparáveis se e só se os vértices correspondentes no grafo são adjacentes. Uma espécie de diagrama de Hasse munido de uma função “indecisão”!

Ainda não chegamos a um estágio ideal da combinatória algébrica que nos permitisse, categoricamente, aderir a certas transferências combinatórias privilegiadas em detrimento de outras. Existe, de maneira subjacente, a questão da moda. Por exemplo, não erraríamos muito ao pronunciar o estudo de estruturas que gozam da propriedade de Cohen-Macaulay como a senha mágica para o reino atual da teoria. Mas, isto pode mudar de curso, a depender das necessidades e precedências de teorias correlatas.

Um aspecto interessante é o de que, apesar de lidar com estruturas finitas, a teoria tem características de tipo infinito quando indaga pelos invariantes e propriedades que estabilizam durante um processo indefinido de transferências combinatórias.

Questões nesta linha são extremamente intrincadas (sem mencionar o problema da complexidade computacional subjacente a muitas delas – vide *Palimpsesto 3*). A descoberta de teoremas de enunciado claro e simples neste emaranhado de relações tem sido objeto de esforço continuado por parte de especialistas em combinatória e, mais recentemente, em álgebra comutativa. Sugerimos a consulta à bibliografia.

CAPÍTULO

**3**

ÁLGEBRA COMUTATIVA, I: O PAPEL  
DOS MONÔMIOS

## Capítulo 3. Álgebra Comutativa, I: O papel dos monômios

### MONÔMIOS: ENCARNAÇÕES

**3.1 Monômios livres de quadrados.** Seja  $E$  uma estrutura combinatoria, montada sobre um conjunto com  $n$  elementos (por exemplo,  $E$  poderia ser um grafo, um conjunto munido de partição, um reticulado, etc.).

Fixando um corpo de base  $k$ , o intérprete típico das propriedades combinatorias de  $E$ , em álgebra, é um conjunto de monômios ou, mais precisamente, de *termos monomiais*.

Lembremos que um monômio sobre  $k$  é um polinômio da forma

$$c_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n},$$

enquanto que o termo monomial (ou, simplesmente, o termo) correspondente é o monômio  $X_1^{i_1} \cdots X_n^{i_n}$ . A distinção entre estas duas noções é imperceptível, especialmente do ponto de vista da teoria dos ideais (mais adiante). Em determinados contextos, ela se torna importante.

Um monômio  $c_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$  – ou o termo correspondente – é dito ser *livre de quadrados* se  $i_l \leq 1$  para todo  $1 \leq l \leq n$ . A filosofia geral é a de que todo problema formulado em termos dos monômios deva ser reduzido a um envolvendo apenas monômios livres de quadrados. O preço a pagar recai, via de regra, no custo da complexidade (leia-se: mais variáveis do que as originais). Este drama, vivido em mais de um contexto, está presente no fenômeno clássico da *polarização*, um dos favoritos da clássica Teoria dos Invariantes.

Felizmente, uma boa parte dos problemas envolvendo grafos e complexos simpliciais se deixam formular através de monômios livres de quadrados. Os monômios gerais continuam a impor sua presença nos cálculos intermediários, mas não como intérpretes diretos.

Para a explicação dos termos correntes em álgebra comutativa, remetemos o leitor à seção Terminologia de Álgebra Comutativa, no final do texto, à qual nos referiremos simplesmente como *Terminologia*.

**3.2 Primeira encarnação: Hodge, álgebras discretas.** A teoria das *álgebras de Hodge* (também chamadas *álgebras com retificação*) foi criada para dar um tratamento uniforme a vários problemas de Álgebra e de Geometria Algébrica que são *governados* por monômios com certa estrutura – os exemplos mais conhecidos sendo as variedades grassmannianas, as variedades schubertianas e os lugares determinantis.

A definição de uma tal álgebra requer os seguintes ingredientes.

- (1) Um conjunto parcialmente ordenado  $H$ ;
- (2) Um conjunto  $\Sigma$  de monômios nos elementos de  $H$ , que é também um *ideal* no sentido de que se  $M \in \Sigma$  e  $N$  é qualquer monômio, então  $MN \in \Sigma$ ;
- (3) O complementar de  $\Sigma$  em  $H$ , constituído dos chamados monômios  $\Sigma$ -básicos (em inglês: *standard*).

Em seguida, é dado um corpo  $k$  (por exemplo,  $\mathbb{Q}$ , se o interesse é puramente combinatório, ou  $\mathbb{R}$ ,  $\mathbb{C}$ , se o objetivo é ultimamente geométrico). Neste contexto, uma *álgebra de Hodge governada por  $\Sigma$*  é um anel  $A$ , contendo  $k$  e  $H$ , gerado pelos elementos de  $H$  sobre  $k$ , satisfazendo a duas condições:

- $H_1$ . Os monômios  $\Sigma$ -básicos constituem uma base para  $A$  como espaço vetorial sobre  $k$ ;
- $H_2$ . Dado um  $M \in \Sigma$  *indivisível* (isto é, não múltiplo próprio de um elemento de  $\Sigma$ ), se

$$(3.2-1) \quad M = \sum_j \lambda_j N_j \quad \lambda_j \neq 0,$$

é a sua expressão na base dos monômios  $\Sigma$ -básicos, então, para todo  $h \in H$  que divide  $M$  e todo  $N_j$ , existe um  $h_j \in H$  dividindo  $N_j$  tal que  $h_j < h$ .

As expressões (3.2-1), para os vários elementos indivisíveis de  $\Sigma$ , são as *relações de retificação* da álgebra de Hodge.

Algumas observações merecem atenção nesta etapa:

- (1) O conjunto  $\Sigma$  é, de fato, um ideal de ordem no conjunto parcialmente ordenado de todos os monômios em  $H$ , cuja ordem é dada pela relação de divisibilidade. A rigor, os monômios nos elementos de um conjunto abstrato  $H$  são os elementos de  $\mathbb{N}^H$ , este ordenado coordenada a coordenada.

- (2) O anel  $A$  não é, em geral, um anel de polinômios nos elementos do conjunto  $H$ ;
- (3) Ainda que os elementos não indivisíveis de  $H$  possam se tornar supérfluos sob vários aspectos da teoria dos anéis, não podem ser descartados do ponto de vista da teoria de Hodge;
- (4) Por trás das duas observações anteriores está a dificuldade de provar que, em qualquer caso, as relações de retificação geram todas as relações de apresentação da álgebra de Hodge (no que pese valer isto em muitas situações importantes);
- (5) Mesmo nos casos em que as relações retificadoras geram todas as outras, elas não constituem sempre uma representação mais econômica possível.

(3.2.1) EXEMPLO. Considere o conjunto

$$H = \{X, Y, Z, XY, XZ\} \subset k[X, Y, Z]$$

(anel de polinômios a três variáveis), parcialmente ordenado da seguinte maneira:

$$Y < Z, \quad XY < X, \quad XZ < X, \quad XY < Y, \quad XZ < Z, \quad XY < XZ.$$

Então o próprio anel  $A = k[X, Y, Z]$  é uma álgebra de Hodge governada pelos monômios  $\Sigma := \{X \cdot Y, X \cdot Z, Y \cdot XZ\}$  (os produtos de dois elementos incomparáveis em  $H$ ), com as relações de retificação

$$(3.2-2) \quad X \cdot Y = 1 \cdot XY, \quad X \cdot Z = 1 \cdot XZ, \quad Y \cdot XZ = 1 \cdot XY \cdot Z.$$

(3.2.2) EXERCÍCIO. No exemplo acima, mostre:

- (i) Os monômios  $\Sigma$ -básicos formam uma base vetorial de  $A$  sobre o corpo  $k$  (*Atenção:  $A$  é um espaço de dimensão infinita!*);
- (ii) As relações de retificação são, de fato, as de (3.2-2);
- (iii) Uma das relações em (3.2-2) é supérflua (isto é, resulta das outras);
- (iv) As relações (3.2-2) apresentam o anel de polinômios  $A$  na forma

$$k[X, Y, Z, T, U]/(XY - T, XZ - U, YT - ZU)$$

cuja economia não é especialmente notável.

O exemplo mais simples de uma álgebra de Hodge é aquele em que as relações de retificação são nulas (isto é, o segundo membro de (3.2-1) é



igual a zero) – neste caso, dizemos que a álgebra é *discreta*. Assim, uma álgebra discreta é da forma  $k[H]/(\Sigma)$ , onde  $(\Sigma)$  designa o ideal do anel  $k[H]$  gerado pelos elementos de  $\Sigma$ . Do ponto de vista das operações de anel, uma álgebra discreta é simplesmente um anel de resíduos de um anel de polinômios relativamente ao ideal gerado por um conjunto de monômios indivisíveis – para obter esta representação, podemos descartar os elementos divisíveis em ambos  $H$  e  $\Sigma$ .

Na verdade, esta estrutura discreta é subjacente a qualquer álgebra de Hodge. De maneira mais ou menos vaga, a estrutura discreta subjacente governa parte dos fenômenos pertinentes à álgebra dada.

(3.2.3) **EXEMPLO.** Descreva a álgebra discreta subjacente ao exemplo acima (*Atenção:* Esta álgebra constitui um dos exemplos mais simples de anel que não é de Cohen–Macaulay - vide *Terminologia*).

**3.3 Segunda: Macaulay.** A concepção de certos anéis através de suas relações de retificação (cf. 3.2), analisada exaustivamente por Hodge no caso clássico dos grassmannianos [HoPe52], tem raízes anteriores, recuando até Macaulay [Mac27].

O trabalho de Macaulay, sob título ligeiramente desconcertante – mas, lembrar que, praticamente até bem final da primeira metade do século, a terminologia algébrica inglesa manteve-se britanicamente isolada do continente – trouxe reflexos, várias décadas mais tarde, para a teoria combinatório-enumrativa dos ideais, num fenômeno típico de “insight” em matemática.

O objetivo desta seção é fornecer algum sabor da concepção de Macaulay, mantendo a simplicidade da exposição. Por outro lado, vale como oportunidade de voltar às definições das seções 1.6 e 3.2.

Consideremos um anel de polinômios  $k[\underline{X}] = k[X_1, \dots, X_n]$  sobre o corpo (fixo)  $k$ . O conjunto  $\mathfrak{M} := \mathfrak{M}(\underline{X})$  dos termos (isto é, dos monômios de coeficiente 1) de  $k[\underline{X}]$  é parcialmente ordenável pela relação de divisibilidade

$$\underline{X}^a \leq \underline{X}^b \Leftrightarrow \underline{X}^a \mid \underline{X}^b.$$

Estaremos interessados, fundamentalmente, em ideais de ordem deste conjunto parcialmente ordenado (cf. 1.6), já utilizados na seção anterior – por conveniência, a relação de ordem nesta seção é a reversa da usada em 3.2, de modo que os ideais de ordem aqui considerados correspondem a filtros lá.

Observemos que  $\mathfrak{M}$  também admite (muitas!) relações de ordem total, compatíveis com sua estrutura de semigrupo multiplicativo, todas transferíveis do semigrupo aditivo  $\mathbb{N}^n$ , através do “logaritmo”

$$\log : \mathfrak{M} \longrightarrow \mathbb{N}^n, \quad \log(\underline{X}^a) = a = (a_1, \dots, a_n).$$

Fixaremos, de uma vez por todas, a ordem total designada como *lexicográfica reversa*, definida da seguinte maneira (digamos, em  $\mathbb{N}^n$ ):  $a = (a_1, \dots, a_n) < b = (b_1, \dots, b_n)$  se e somente se  $\sum a_i < \sum b_i$  ou  $\sum a_i = \sum b_i$ , em cujo caso exige-se que  $a_n = b_n, \dots, a_{j+1} = b_{j+1}, a_j < b_j$  para algum  $j$  tal que  $1 \leq j \leq n$ .

Um dos resultados básicos de Macaulay tira proveito da interação entre a ordem lexicográfica reversa de  $\mathfrak{M}$  e sua ordem parcial de divisibilidade. Para entender o alcance desta interação, introduzimos a idéia de estrutura graduada.

(3.3.1) DEFINIÇÃO. Seja  $(d_1, \dots, d_n) \in \mathbb{N}^n$ . O anel de polinômios graduado munido de tara  $(d_1, \dots, d_n)$  é o anel  $k[\underline{X}]$ , com a variável  $X_i$  rotulada pelo peso ou grau  $d_i$ . O peso de um monômio  $\underline{X}^a = X_1^{a_1} \dots X_n^{a_n}$  relativamente à tara  $(d_1, \dots, d_n)$  é o inteiro  $\sum a_i d_i$ . Um ideal  $I \subset k[\underline{X}]$  é dito *quase-homogêneo* se existe uma tara  $(d_1, \dots, d_n)$  de  $k[\underline{X}]$  e um sistema de geradores  $f_1, \dots, f_m$  de  $I$  tal que, para todo  $j = 1, \dots, m$ , os monômios de  $f_j$  têm todos o mesmo peso relativamente à tara  $(d_1, \dots, d_n)$ . Se  $I \subset k[\underline{X}]$  é um ideal quase-homogêneo relativamente a uma certa tara, dizemos que o anel de resíduos  $k[\underline{X}]/I$  é *graduado* (relativamente àquela tara).

Uma suposição permanente será a de que todos os ideais considerados estarão tacitamente contidos no ideal máximo gerado pelas variáveis  $\underline{X}$ .

(3.3.2) EXERCÍCIO. Sejam  $a > b > c > 0$  inteiros tais que  $\text{mdc}(a, b, c) = 1$  e sejam  $t$  e  $X, Y, Z$  conjuntos de variáveis sobre o corpo  $k$ . Mostre que o núcleo do homomorfismo (cf. *Terminologia*) definido por

$$k[X, Y, Z] \longrightarrow k[t], \quad X \mapsto t^a, Y \mapsto t^b, Z \mapsto t^c$$

é um ideal quase-homogêneo com tara  $(a, b, c)$ .

Eis o resultado de Macaulay.

(3.3.3) TEOREMA. (Teorema menor de Macaulay) Seja  $A := k[\underline{X}]/I$  um anel graduado. Então existe um ideal de ordem em  $\mathfrak{M}$  cujos resíduos constituem uma  $k$ -base vetorial de  $A$ .

DEMONSTRAÇÃO: Denotemos  $\leq$  a ordem total lexicográfica reversa em  $\mathfrak{M}$ . Consideremos um subconjunto de  $\mathcal{J} \subset \mathfrak{M}$  definido, por recorrência, da seguinte maneira:

- (1)  $1 \in \mathcal{J}$ .
- (2) Se  $M_1, \dots, M_i \in \mathcal{J}$ , então  $M_{i+1}$  é o menor elemento de  $\mathfrak{M}$ , na ordem  $\leq$ , tal que os resíduos de  $M_1, \dots, M_i, M_{i+1}$  em  $A$  são linearmente independentes.

Deixamos ao leitor a incumbência de mostrar que os resíduos de  $\mathcal{J}$  geram  $A$  como espaço vetorial, usando a estrutura graduada subjacente.

Afirmamos que  $\mathcal{J}$  é um ideal de ordem do conjunto parcialmente ordenado  $\mathfrak{M}$  (na ordem parcial da divisibilidade). Com efeito, se assim não fosse, existiriam  $M, N \in \mathfrak{M}$ , tais que  $M \in \mathcal{J}$ ,  $N \mid M$  e  $N \notin \mathcal{J}$ . Ora, sendo os resíduos de  $\mathcal{J}$  uma base de  $A$ , devemos ter uma relação de dependência linear

$$(3.3-1) \quad N - \sum_{M_i \in \mathcal{J}} \lambda_i M_i \in I,$$

com  $M_i < N$  (porque?). Por outro lado, temos  $M = NL$ , para algum  $L \in \mathfrak{M}$ . Multiplicando a relação (3.3-1) por  $L$ , resulta  $M - \sum \lambda_i (M_i L) \in I$ . Mas,  $\leq$  é compatível com o produto de termos; logo,  $M_i L < NL = M$ . Contudo, isto seria uma contradição, uma vez que, pela construção de  $\mathcal{J}$ , o resíduo de  $M \in \mathcal{J}$  não pode ser combinação linear de resíduos anteriores. ■

Uma ordem  $\leq$  tal como consideramos aqui é um exemplo das chamadas *ordens de termos* que respeitam o grau total dos termos. Tais ordens são essenciais para a teoria e a implementação algorítmica das bases de Gröbner (cf. *Palimpsesto 1*).

A designação “teorema menor” será esclarecida à luz das seções 3.6 e 3.7, onde o papel dos ideais de ordem terá um relevo especial.

**3.4 Terceira: Hironaka, Rees, outros.** O teorema menor de Macaulay, juntamente com a idéia de *retificação* introduzida na seção 3.2, deixam aparente a riqueza da estrutura vetorial de um anel graduado  $k[\underline{X}]/I$ . No

fundo, o que isto nos revela é que a estrutura vetorial de tais anéis admite muitas decomposições em somas diretas de subespaços e que estas decomposições têm características combinatórias notáveis.

O objetivo desta seção é dar um pouco mais de transparência a esta idéia. Para iniciar, daremos um exemplo no contexto dos chamados *ideais determinantis*.

(3.4.1) DEFINIÇÃO. Seja  $k$  um corpo e  $\underline{X} := X_{ij}$ ,  $1 \leq i \leq n$ ,  $1 \leq j \leq m$ , indeterminadas sobre  $k$ . O sub-determinante de  $\underline{X}$  formado pelas linhas  $l_1, \dots, l_s$  e pelas colunas  $p_1, \dots, p_s$  será denotado por  $[l_1 \dots l_s \mid p_1 \dots p_s]$ . Uma *bi-tabela* (de Young) é um produto

$$B = [l_{11} \dots l_{1s_1} \mid p_{11} \dots p_{1s_1}] \cdots [l_{t1} \dots l_{ts_t} \mid p_{t1} \dots p_{ts_t}]$$

satisfazendo as condições

$$s_1 \geq s_2 \geq \dots \geq s_t, \quad l_{ij} < l_{i,j+1}, \quad p_{ij} < p_{i,j+1}$$

para todas as escolhas de  $i, j$ . O comprimento  $\lambda(B)$  da bi-tabela  $B$  é o inteiro  $s_1$ ;  $B$  é dita *básica* (“standard”) se  $l_{ij} \leq l_{i+1,j}$  e  $p_{ij} < p_{i+1,j}$ , para todos  $i, j$ .

(3.4.2) TEOREMA. [DoRoSt74] Toda bi-tabela  $B \in k[\underline{X}]$  é uma combinação  $k$ -linear  $B = \sum \alpha_i B_i$  satisfazendo as condições

- (1)  $B_i$  é básica para todo  $i$ ;
- (2)  $B$  e  $B_i$  têm o mesmo grau (como polinômios homogêneos), para todo  $i$ ;
- (3)  $\lambda(B_i) \geq \lambda(B)$  para todo  $i$ .

A teoria das bi-tabelas tem sido estudada intensamente, não só do ponto de vista combinatório, mas também sob o enfoque da teoria dos invariantes [DeKuRo78] e da álgebra comutativa e geometria algébrica [CoEiPr82].

Para enunciar o próximo resultado, usamos a noção de *largura*  $l(M)$  de um termo  $M \in \mathfrak{M}(\underline{X})$ . A saber, escrevemos  $M = \prod_{i=1}^d X_{l_i, p_i} = \prod_i [l_i \mid p_i]$ , onde  $l_1 \leq \dots \leq l_d$  e  $p_i \leq p_{i+1}$  sempre que  $l_i = l_{i+1}$ . Então,  $l(M)$  é o comprimento da mais longa sub-sequência estritamente decrescente do conjunto  $\{p_1, \dots, p_d\}$ .

(3.4.3) TEOREMA. [Sch61], [Knu70] Seja  $\mathfrak{B}$  o conjunto das bi-tabelas em  $k[\underline{X}]$ . Existe uma bijeção

$$\mathfrak{k} : \mathfrak{M} \longrightarrow \mathfrak{B}$$

tal que, para todo  $M \in \mathfrak{M}$ ,  $M$  e  $\mathfrak{k}(M)$  têm o mesmo grau e a mesma largura.

O anel determinantal de ordem  $r$  é o anel de resíduos  $k[\underline{X}]/I_r$ , onde  $I_r = I_r(\underline{X})$  é o ideal gerado pelos sub-determinantes  $r \times r$  de  $\underline{X}$ . É evidente que se trata de um anel homogêneo.

(3.4.4) PROPOSIÇÃO. Seja  $A_r$  o anel determinantal de ordem  $r$ . Vale

$$\dim_k(A_r)_d = \#\{M \in \mathfrak{M} \mid \text{grau } M = d \text{ e } l(M) \leq r - 1\}$$

onde  $(A_r)_d$  denota o subespaço vetorial de  $A_r$  constituído pelos resíduos dos polinômios homogêneos de grau  $d$ .

O exemplo seguinte aparece em [Stu90a], tendo sido calculado numa implementação de bases de Gröbner, usando o sistema MAPLE.

(3.4.5) EXEMPLO. Seja  $(\underline{X})$  uma matriz  $5 \times 5$  e  $r = 3$ . Na base dos termos de largura  $\leq 2$ , o monômio  $X_{15}X_{24}X_{33}X_{42}X_{51}$  tem uma expressão consistindo de 28 termos. Eis os 11 primeiros termos desta expansão:

$$\begin{aligned} & 3X_{11}X_{22}X_{33}X_{44}X_{55} - 2X_{11}X_{22}X_{33}X_{45}X_{54} - 3X_{11}X_{22}X_{34}X_{43}X_{55} \\ & + X_{11}X_{22}X_{34}X_{45}X_{53} + X_{11}X_{22}X_{35}X_{43}X_{54} - 3X_{11}X_{23}X_{32}X_{44}X_{55} \\ & + 2X_{11}X_{23}X_{32}X_{45}X_{54} + 2X_{11}X_{23}X_{34}X_{42}X_{55} - X_{11}X_{23}X_{34}X_{45}X_{52} \\ & \quad + 2X_{11}X_{24}X_{32}X_{45}X_{55} - X_{11}X_{24}X_{35}X_{42}X_{53} - \dots \end{aligned}$$

(3.4.6) EXERCÍCIO. Quais os termos restantes da expansão acima? (O leitor terá de escrever seu próprio programa).

A decomposição específica para anéis determinantis resulta de sua natureza de álgebra com retificação. Para um anel graduado da forma  $k[\underline{X}]/I$ , mas arbitrário, ainda é possível obter uma decomposição em soma direta de subespaços vetoriais, embora de maneira mais frouxa.

Esta decomposição mais geral ficou conhecida na literatura como *decomposição de Hironaka-Rees*. A idéia apareceu, pela primeira vez, num trabalho de Rees [Ree56], tendo sido reelaborada e generalizada por vários

autores, destacando-se entre estes Baclawski e Garsia [Gar80], [BaGa81], [Bac81a].

É de algum interesse observar que, tendo se originado por razões teóricas e sido usada para extrair consequências teóricas (vide 4.1 e 4.2), esta decomposição venha mostrando eficiência do ponto de vista computacional (cf., por exemplo, [StWh90])

Baclawski e Garsia deram o seguinte formato ao teorema de decomposição.

(3.4.7) TEOREMA. ([BaGa81]) *Seja  $A := k[X]/I$  um anel graduado de dimensão  $d$ . Então  $A$  admite um sistema de parâmetros  $\theta_1, \dots, \theta_d$  e uma sequência de elementos homogêneos  $\eta_1, \dots, \eta_m$  tais que*

(i) *Os resíduos de  $\eta_1, \dots, \eta_m$  em  $A/(\theta_1, \dots, \theta_d)$  constituem uma base deste como  $k$ -espaço vetorial.*

(ii) *Existe uma função  $k : \{1, \dots, m\} \rightarrow \{0, 1, \dots, r\}$  tal que todo elemento de  $A$  admite uma expressão única da forma*

$$\sum_{j=1}^m \eta_j p_j(\theta_1, \dots, \theta_{k(j)}),$$

onde  $p_j \in k[X_1, \dots, X_{k(j)}]$ .

(iii)  $\eta_j(\theta_{k(j)+1}, \dots, \theta_d) \subset (\theta_1, \dots, \theta_{k(j)})$ , para todo  $j = 1, \dots, m$ .

Os elementos  $\eta_1, \dots, \eta_m$  são chamados *separadores* e a função  $k$ , a *separatriz*, da decomposição. A demonstração de (3.4.7), assim como a do teorema original de Rees, baseia-se num processo de indução mais ou menos padronizado, mas trabalhoso.

Através da decomposição de Hironaka–Rees, é possível antecipar o *début* dos anéis de Cohen–Macaulay. Estes serão o principal tema do capítulo seguinte, mas um exemplo já apareceu nesta seção: os anéis determinantis.

(3.4.8) PROPOSIÇÃO. *As seguintes condições são equivalentes para um anel graduado  $A$  de dimensão  $d$ :*

(i)  *$A$  admite um sistema de parâmetros e uma sequência de separadores para os quais a função separatriz assume valores constantes iguais a  $d$ .*

(ii)  *$A$  admite um sistema de parâmetros que é uma  $A$ -sequência.*

(3.4.9) OBSERVAÇÃO. Conforme foi mencionado mais acima, a intenção original da decomposição de Hironaka–Rees era teórica. Baclawski e Garsia

aplicaram-na para obter informação sobre os detalhes da transferência

$$\Delta \rightsquigarrow \Delta_c(\Delta)$$

que associa a um complexo simplicial o complexo simplicial das cadeias do conjunto parcialmente ordenado subjacente de  $\Delta$  (vide 2.5). Voltaremos a este resultado na seção 4.1, após havermos introduzido o anel das faces de um complexo simplicial. A razão de insistirmos no significado algébrico desta transferência reside no fato de que, como vimos em (2.5.12), o complexo  $\Delta_c(\Delta)$  é grafal, logo, em princípio, mais simples do que  $\Delta$ . Esta simplicidade não deve, contudo, ser tomada ao pé da letra, já que  $\Delta_c(\Delta)$  corresponde à divisão baricêntrica de  $\Delta$  (vide 2.5.11), portanto introduz uma complexidade adicional em termos do número de faces.

### ANEIS DE FACES E ARESTAS

Chegou a ocasião de colocar em prática o principal objetivo do curso, qual seja o de formular propriedades de entes combinatórios em termos de anéis definidos por monômios. As palavras-chave combinatórias são: grafos, complexos simpliciais e conjuntos parcialmente ordenados - além de suas versões mais geométricas, tais como os politopos.

A idéia de associar monômios a estruturas combinatórias não é tão recente, se bem que nem sempre muito explícita. Esta idéia está por trás de procedimentos na teoria clássica dos invariantes. Pelo menos num trabalho datado do século passado, encontramos resquícios desta associação (vide [Pet891]). É provável, senão certo, que uma busca mais cuidadosa na literatura clássica localize outras tentativas semelhantes.

Contudo, somente mediante a ferramenta mais poderosa da combinatória moderna e da álgebra tornou-se possível um tratamento sistemático desta idéia. Atualmente, a multiplicidade existente de tratamentos monomiais de estruturas combinatórias faz perder de vista os objetivos, tornando-se extremamente difícil para o leitor inexperiente entender os resultados.

Nos parágrafos que se seguem, procuraremos tornar mais palpáveis algumas dessas associações monomiais, através de dois exemplos particulares: grafos e complexos simpliciais. Estes exemplos não são, necessariamente, os mais simples ou naturais (politopos teriam precedência, talvez). Mas, pelo menos saem com a vantagem de que conceitos razoavelmente sofisticados de álgebra comutativa são imediatamente aplicáveis.

### 3.5 O anel de Petersen. Ideais de arestas.

Seja  $G = (\mathcal{V}, \mathcal{A})$  um grafo;  $k$  designará um corpo, fixo de uma vez por todas. Consideremos uma bijeção ordenada  $v_i \leftrightarrow X_i$  entre o conjunto dos vértices de  $G$  e um conjunto  $\underline{X} = \{X_1, \dots, X_n\}$  de indeterminadas sobre  $k$ .

(3.5.1) DEFINIÇÃO. O ideal das arestas de  $G$  é o ideal  $I(G) \subset k[\underline{X}]$  gerado pelos monômios  $X_i X_j$  tais que  $(v_i, v_j) \in \mathcal{A}$ . O anel das arestas ou anel de Petersen de  $G$  é o anel residual  $k[G] := k[\underline{X}]/I(G)$ .

O anel de Petersen codifica as informações essenciais do grafo. Esta codificação não é sempre fácil de precisar e, evidentemente, não funciona no sentido contrário (por exemplo, qual o significado, na teoria dos grafos, da soma de “arestas” em  $I(G)$ ?). Mas, como veremos, suscita problemas curiosos.

A codificação tende a funcionar de maneira exata, mais para “coleções” do que para “indivíduos”.

(3.5.2) PROPOSIÇÃO. A bijeção entre  $\mathcal{V}(G)$  e  $\underline{X}$  induz uma bijeção entre a coleção das coberturas de vértices de  $G$  e a coleção de ideais de  $k[\underline{X}]$  da forma  $(X_{i_1}, \dots, X_{i_p})$ , contendo  $I(G)$ .

A proposição resulta, imediatamente, das definições. Ela admite um grau de precisão adicional, a saber, a bijeção induzida é um isomorfismo entre as estruturas naturais de conjuntos parcialmente ordenados das duas coleções. Em particular, as coberturas mínimas de  $G$  correspondem aos ideais gerados por variáveis que são ideais mínimos do ideal  $I(G)$  (vide *Terminologia*).

(3.5.3) EXERCÍCIO. Torne explícita a correspondência acima para vários dos exemplos de grafos já considerados no texto.

Uma das propriedades básicas do ideal das arestas de um grafo é comum a todos os ideais gerados por monômios livres de quadrados.

(3.5.4) PROPOSIÇÃO. Se  $I \subset k[\underline{X}]$  é um ideal gerado por monômios livres de quadrados, então  $I$  é radical (vide *Terminologia*).

DEMONSTRAÇÃO: Seja  $f \in k[\underline{X}]$  tal que  $f^l \in I$ . Como  $I$  é gerado por monômios, podemos supor (porque?) que todo monômio de  $f^l$  pertence a  $I$ . Seja, então,  $X_1^{r_1} \cdots X_n^{r_n}$  um monômio típico de  $f$ . Por hipótese,  $X_1^{r_1 l} \cdots X_n^{r_n l}$  é divisível por um monômio livre de quadrados pertencente a  $I$ . Segue-se que o próprio  $X_1^{r_1} \cdots X_n^{r_n}$  já é divisível por este monômio, logo,  $f \in I$ . ■



(3.5.5) COROLÁRIO. O ideal das arestas de  $G$  é a interseção dos ideais primos da forma  $(X_{i_1}, \dots, X_{i_p})$  correspondentes às coberturas mínimas de vértices de  $G$ .

(3.5.6) EXERCÍCIO. Mostre, por meio de exemplo, que a interseção de uma coleção de ideais gerados por vértices de um grafo não é, em geral, um ideal de arestas de algum subgrafo.

(3.5.7) EXERCÍCIO. Seja  $G$  um grafo e  $\mathcal{U} \subseteq \mathcal{V}(G)$ . Seja  $\mathcal{C}$  uma coleção de subconjuntos de  $\mathcal{U}$  satisfazendo as seguintes condições:

- (i)  $\bigcup_{V \in \mathcal{C}} V = \mathcal{U}$ ;
- (ii) Conjuntos distintos da coleção  $\mathcal{C}$  são incomparáveis por inclusão;
- (iii) Para todo  $v_i \in \mathcal{U}$ , existe algum  $v_{j(i)} \in \mathcal{U}$  satisfazendo a seguinte propriedade: se  $V \in \mathcal{C}$  é tal que  $v_i \notin V$ , então  $v_{j(i)} \in V$ .

Mostre:

- (1) A interseção dos ideais (primos) gerados pelos conjuntos pertencentes a  $\mathcal{C}$  é o ideal das arestas de um subgrafo de  $G$ .
- (2) Nenhuma das condições acima pode ser omitida (dê exemplos).

### Dimensão e número de cobertura.

(3.5.8) PROPOSIÇÃO. Para um grafo  $G$  vale:

- (i) A altura (cf. Terminologia) do ideal  $I(G)$  é igual a  $\alpha_0(G)$  (vide 2.1).
- (ii) A dimensão (cf. Terminologia) do anel de Petersen  $k[G]$  é igual a  $\beta_0(G)$  (vide 2.2).

DEMONSTRAÇÃO: Exercício.

O que dizer da profundidade (cf. Terminologia) do anel de Petersen? Infelizmente, trata-se de um problema difícil, não sendo óbvio se a profundidade é um invariante combinatório do grafo.

(3.5.9) EXERCÍCIO. (i) Mostre que toda variável  $X_i$ , correspondente a um vértice não isolado do grafo  $G$ , é um divisor de zero no anel de Petersen  $k[G]$ .

(ii) Determine seqüências regulares máximas (cf. Terminologia) para os anéis de Petersen dos grafos  $C_n$ , ( $n \leq 6$ ).

(iii) Determine uma seqüência regular máxima de  $k[\underline{X}]$  contida no ideal das arestas do grafo  $K_n$ .

## O problema da funtorialidade do anel de Petersen

Por funtorialidade de uma associação entre os objetos de duas categorias entendemos, em geral, uma associação, naturalmente induzida, entre os morfismos das duas categorias.

No nosso caso temos, de um lado os morfismos de grafos (vide 1.2); de outro, os homomorfismos de anéis residuais dos vários anéis de polinômios  $k[X]$ . Como um morfismo de grafos  $\varphi : G \rightarrow H$  tem uma aplicação subjacente a nível de vértices, êle induz naturalmente um homomorfismo entre os anéis de polinômios, no sentido covariante:

$$\varphi_* : k[X] \rightarrow k[Z].$$

A dificuldade em obter um homomorfismo covariante, a nível dos anéis de Petersen, reside na possibilidade de colapso, isto é, de  $\varphi$  não ser injetora.

Uma alternativa para resolver o impasse é simplesmente desconhecer a existência de técnicas indutivas importantes na teoria dos grafos, que dependem sistematicamente do “colapso” de vértices ou de “contração” de arestas, e supor que todo morfismo de grafos é injetor.

A segunda alternativa, talvez mais sensata, baseia-se no processo de “omissão de laços”. Para descrever este processo, ressuscitemos, temporariamente, os *relmultigrafos*, isto é, os grafos em que laços e arestas múltiplas coexistem, harmoniosamente, com as arestas “honestas”.

Definamos o anel de Petersen generalizado para um relmultigrafo, de modo completamente análogo: a diferença, como se percebe, é que, desta feita, temos de conviver com um ideal de arestas que admite geradores da forma  $X_i^m X_j^m$  (com a possibilidade de que  $X_i = X_j$ ).

Deixamos ao leitor a tarefa de colocar nos trilhos a afirmação seguinte: existe uma correspondência natural entre morfismos de relmultigrafos – definidos de maneira completamente paralela à dos grafos simples – e homomorfismos dos anéis de Petersen generalizados.

Esta generalização não resolve o problema original, uma vez que a restrição desta associação aos grafos simples tem imagem “desonesta” – mas, insinua uma tática. Esta tática é, *per forza*, não funtorial.

(3.5.10) DEFINIÇÃO. Seja  $G$  um grafo e  $(v_1, v_2) \in \mathcal{A}(G)$ , uma aresta de  $G$ . A *contração de*  $(v_1, v_2)$  é o grafo  $G/(v_1, v_2) := (\mathcal{W}, \mathcal{B})$  definido pelas seguintes regras:

(i)  $\mathcal{W}$  é a reunião disjunta de  $\mathcal{V}(G) \setminus \{v_1, v_2\}$  com um vértice  $v$  (pensamos

em  $v$  como sendo obtido por identificação dos vértices  $v_1$  e  $v_2$ );  
(ii)  $\mathcal{B}$  é a reunião dos conjuntos

$$\mathcal{A} \cap ((\mathcal{V}(G) \setminus \{v_1, v_2\}) \times (\mathcal{V}(G) \setminus \{v_1, v_2\}))$$

e

$$\{(v, w) \mid w \in \mathcal{V}(G) \setminus \{v_1, v_2\} \text{ com } (v_1, w) \in \mathcal{A} \text{ ou } (v_2, w) \in \mathcal{A}\}.$$

Deixamos ao leitor a tarefa de verificar que, para cada  $(v_1, v_2)$ , só existe um grafo (a menos de isomorfismos) com estas propriedades.

(3.5.11) EXERCÍCIO. Seja  $\varphi : G \rightarrow H$  um morfismo de grafos.

(i) Mostre que  $\varphi$  induz um morfismo de um grafo obtido de  $G$ , por contração de arestas, em  $H$  e que este homomorfismo dá lugar a um homomorfismo dos anéis de Petersen respectivos.

(ii) Dê uma explicação do homomorfismo induzido em termos do núcleo do homomorfismo  $\varphi_* : k[X] \rightarrow k[Z]$  a nível dos anéis de polinômios originais.

Além da contração de arestas, outro procedimento indutivo importante na teoria dos grafos é o da *remoção* de vértices já mencionado anteriormente (vide 2.1). Deixamos ao leitor a verificação de que, dado um grafo  $G$  e um vértice  $v \in G$ , então a operação de passar de  $G$  a  $G - v$  corresponde, a nível dos anéis de Petersen respectivos, ao homomorfismo induzido pela “avaliação”  $v = 0$ . Esta interpretação não é, contudo, exata (porque?).

Finalmente, um morfismo de grafos que induz um homomorfismo natural é a injeção de um subgrafo num grafo. Esta afirmação, cuja veracidade pode ser facilmente suprida pelo leitor, admite o seguinte suplemento.

(3.5.12) PROPOSIÇÃO. Se  $G$  é um grafo e  $H$ , um subgrafo de  $G$ , então o homomorfismo de anéis  $k[H] \rightarrow k[G]$  induzido pela inclusão de  $\mathcal{V}(H) \subset \mathcal{V}(G)$  é injetor se e somente se  $H$  é um subgrafo induzido.

DEMONSTRAÇÃO: Lembramos que um subgrafo  $H$  é induzido se toda aresta de  $G$  cujos vértices (ambos) pertencem a  $\mathcal{V}(H)$ , já pertence a  $H$ . Ora, o homomorfismo induzido a nível dos anéis de Petersen é injetor se e só se

$$I(G) \cap k[X_{i_1}, \dots, X_{i_m}] = I(H)$$

onde  $\{X_{i_1}, \dots, X_{i_m}\}$  corresponde aos vértices de  $H$ . Uma das inclusões é trivial. Para a outra, seja  $f \in I(G) \cap k[X_{i_1}, \dots, X_{i_m}]$ . Podemos supor que  $f$  é um monômio, em cujo caso  $f$  tem de ser divisível por uma aresta de  $G$ . Logo, esta aresta tem de admitir ambos os vértices no subgrafo  $H$ , que é o que queríamos demonstrar. ■

(3.5.13) OBSERVAÇÃO. Se o homomorfismo induzido  $k[H] \rightarrow k[G]$  é injetor, então temos  $\dim k[H] \leq \dim k[G]$ , o que reformula a conhecida relação entre conjuntos independentes de  $G$  e do subgrafo induzido  $H$ .

(3.5.14) EXERCÍCIO. Mostre, por meio de exemplo, que a igualdade

$$\dim k[H] = \dim k[G]$$

pode ter lugar para um subgrafo induzido próprio.

(3.5.15) EXERCÍCIO. Mostre que, para qualquer vértice  $v$  de um grafo  $G$ , o subgrafo  $G - v$  é induzido e que o homomorfismo induzido pela inclusão, composto com o induzido pela avaliação  $v = 0$ , é o homomorfismo idêntico do anel  $k[G - v]$ .

Fica claro que a associação entre grafos e anéis de arestas não é funtorial, mas vários procedimentos contornam esta deficiência, indicando, de resto, que a transferência algébrica pode provocar questões mais difíceis do que as definições deixam crer.

### Estimativas locais.

O problema de estabelecer cota superior para o número de arestas de um grafo, em termos de invariantes do grafo, é um tópico tradicional na teoria dos grafos. Um tanto imprecisamente, diremos que o resultado a seguir é uma contribuição ao repertório de “estimativas locais” do número de arestas.

(3.5.16) PROPOSIÇÃO. Se  $T$  é uma árvore, então vale

$$\mu(I(T)_P) \leq \max\{\text{alt } P - 1, \text{alt } I(G)_P\}$$

para todo ideal primo  $P \subset k[X]$ .

DEMONSTRAÇÃO: A demonstração é por indução no número de vértices da árvore. Rotulando novamente os vértices de  $T$ , se necessário, podemos supor que  $X_n$  é um vértice terminal (isto é, livre) e que  $X_{n-1}$  é o único vértice de  $T$  adjacente a  $X_n$ . Ponhamos  $T' := T - X_n$ ,  $A' := k[X_1, \dots, X_{n-1}]$ ,  $I' := I \cap A'$  and  $P' := P \cap A'$ . Temos, certamente,  $I = (I', X_{n-1}X_n)$  logo,  $\mu(I_P) \leq \mu(I'_{P'}) + 1$ .

Consideremos, primeiramente, o caso em que  $P$  contém  $X_n$ , de sorte que  $P = (P', X_n)$ . Como  $\text{alt } P = \text{alt } P' + 1$ , resulta pela hipótese indutiva

$$\begin{aligned} \mu(I_P) &\leq \mu(I'_{P'}) + 1 \\ &\leq \max \{ \text{alt } P' - 1, \text{alt } I'_{P'} \} + 1 \\ &= \max \{ \text{alt } P - 2, \text{alt } I_P \} + 1. \end{aligned}$$

Desta forma, termina o argumento, a menos que  $\text{alt } I_P = \text{alt } I'_{P'}$ , e  $\text{alt } I'_{P'} > \text{alt } P' - 1$ . Mas, se este for o caso, mostremos que tem-se, na verdade,  $I_P = I'_{P'}$ . De fato, observemos de início que  $P'$  é necessariamente um ideal primo mínimo de  $I'$ . Além disso, ele é obrigado a conter o vértice  $X_{n-1}$ , pois, do contrário, por localização em  $P$ , inverteríamos esta variável, fornecendo  $X_n \in I_P$ , o qual é não divisor de zero sobre o ideal  $I'_{P'}$ ; mas isto contradiz a igualdade  $\text{alt } I_P = \text{alt } I'_{P'}$ . Em seguida, como  $P'$  é um primo correspondente a uma cobertura de vértices mínima de  $T$  que contém o vértice  $X_{n-1}$ , segue-se que algum vértice  $X_{n-3}$  adjacente a  $X_{n-1}$  em  $T$  não pertence  $P'$ . Novamente, localizando em  $P$ , obtemos então  $X_{n-1} \in I'_{P'}$ , conseqüentemente  $I_P = (I', X_{n-1}X_n)_P = I'_{P'}$ , como se pretendia.

Finalmente, consideremos o segundo caso, isto é, em que  $X_n \notin P$ . Neste caso,  $I_P = (I', X_{n-1})_P$  e, como algum vértice distinto de  $X_n$  é adjacente a  $X_{n-1}$ , a aresta correspondente torna-se supérflua. Isto significa, mais uma vez, que se tem  $\mu(I_P) = \mu(I'_{P'})$  e a conclusão segue de maneira análoga, uma vez que, de todas as maneiras,  $\text{alt } P' \leq \text{alt } P$ . ■

**3.6 O anel de Stanley–Reisner.** A codificação algébrica de um complexo simplicial pode, inicialmente, se processar como no caso de um grafo. Primeiramente, estabelecemos uma bijeção ordenada entre o conjunto dos vértices do complexo simplicial  $\Delta$  e um conjunto de indeterminadas  $\underline{X} : X_1, \dots, X_n$  sobre um corpo (fixo)  $k$ .

Em seguida, queremos introduzir um ideal do anel  $k[\underline{X}]$  que reflita propriedades de  $\Delta$ . Após vencer o primeiro impulso de fazer corresponder monômios às faces de  $\Delta$  (porque isto não funcionaria?), optamos pela seguinte:

(3.6.1) DEFINIÇÃO. O *anel das faces*, ou *anel de Stanley-Reisner*, de  $\Delta$  é o anel de resíduos

$$k[\Delta] := k[\underline{X}]/I_\Delta$$

onde  $I_\Delta$  é gerado pelos monômios cujos suportes *não* são faces de  $\Delta$ .

Lembramos que o suporte  $\text{Sup}(\underline{X}^a)$  de um monômio

$$\underline{X}^a = X_1^{a_1} \cdots X_n^{a_n}$$

é o conjunto  $\{X_i \mid a_i \neq 0\}$ .

A primeira Observação é que o ideal das faces  $I_\Delta$  é gerado, minimamente, por monômios livres de quadrados. A segunda, é que  $I_\Delta$  é mais complexo do que um ideal de Petersen, uma vez que seus geradores podem ter graus diversos e maiores do que 2.

A um primeiro contato, a definição de  $k[\Delta]$  é decepcionante, já que o complexo simplicial das faces de um  $n$ -simplexo é o anel de polinômios  $k[X]$ ! Refletindo melhor, o leitor achará esta codificação natural: ela explica a trivialidade do complexo simplicial das faces de um simplexo na teoria simplicial (ou topológica), onde ele, não admite, por exemplo, obstrução homológica.

A Figura 3.1 mostra dois complexos simpliciais que convém manter como modelos da teoria. Ambos aparecem, de maneira recorrente, na literatura [Sta83, Chapter II], [Rei76].

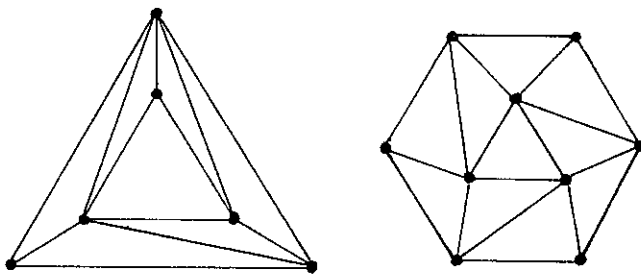


Fig. 3.1: Triangulações de  $S^2$  e de  $\mathbb{P}_{\mathbb{R}}^2$

(3.6.2) EXERCÍCIO. Determine um conjunto de geradores mínimos de  $I_\Delta$ , no caso em que  $\Delta$  é qualquer dos complexos simpliciais da Figura 3.1.

(3.6.3) PROPOSIÇÃO. Seja  $\Delta$  um complexo simplicial. Os resíduos em  $k[\Delta]$  dos elementos de

$$\mathcal{F}(\Delta) := \{\underline{X}^a \mid \text{Sup}(\underline{X}^a) \in \Delta\}$$

constituem uma  $k$ -base vetorial de  $k[\Delta]$ .

DEMONSTRAÇÃO: Primeiro, os resíduos de  $\mathcal{F}(\Delta)$  são linearmente independentes sobre  $k$ . Com efeito, dada uma relação

$$\sum_{\mathcal{F}(\Delta)} \lambda_a \underline{X}^a \in I_\Delta,$$

como  $I_\Delta$  é gerado por monômios, resulta que

$$\lambda_a \neq 0 \Rightarrow \underline{X}^a \in I_\Delta \Rightarrow \text{Sup}(\underline{X}^a) \notin \Delta.$$

Mas, isto é uma contradição. Logo,  $\lambda_a \neq 0, \forall a$ .

Deixamos ao leitor a tarefa de mostrar que os resíduos de  $\mathcal{F}(\Delta)$  geram  $k[\Delta]$  como espaço vetorial sobre  $k$ . ■

(3.6.4) OBSERVAÇÃO. O lema é um caso especial do lema de Macaulay (Capítulo 2, 2.2).

(3.6.5) COROLÁRIO. Se  $\Delta$  é um complexo simplicial e  $F \in \Delta$ , então os resíduos dos vértices de  $F$  são algebricamente independentes sobre  $k$ .

DEMONSTRAÇÃO: Seja  $F = \{X_{i_1}, \dots, X_{i_d}\} \in \Delta$ . Como na argumentação da prova anterior, temos que uma relação polinomial entre estes vértices, digamos,

$$\sum \lambda_a X_{i_1}^{a_{i_1}} \dots X_{i_d}^{a_{i_d}} \in I_\Delta,$$

com algum  $\lambda_a \neq 0$ , acarretaria  $X_{i_1}^{a_{i_1}} \dots X_{i_d}^{a_{i_d}} \in I_\Delta$ . Mas, neste caso, teríamos, novamente, a contradição  $F = \{X_{i_1}, \dots, X_{i_d}\} \notin \Delta$ . ■

(3.6.6) COROLÁRIO. Se  $\Delta$  é um complexo simplicial, vale  $\dim k[\Delta] = \dim \Delta + 1$ .

(3.6.7) EXERCÍCIO. Seja  $\Delta$  um complexo simplicial.

(i) Mostre que existe um conjunto de variáveis  $X_{j_1}, \dots, X_{j_i}$  tal que

$$\dim k[\Delta] = \dim k[\underline{X}]/P,$$

onde  $P = (X_{j_1}, \dots, X_{j_i})$ .

(ii) Sejam  $X_{j_1}, \dots, X_{j_i}$  como em (i). Mostre que o conjunto complementar

$X \setminus \{X_{j_1}, \dots, X_{j_i}\}$  é uma face de  $\Delta$ .

(iii) Deduza, a partir de (ii), uma outra demonstração do Corolário (3.6.6).

A funtorialidade da associação  $\Delta \rightsquigarrow k[\Delta]$  é ainda mais precária aqui do que no caso de grafos. Observemos que, na situação de complexos simpliciais, não existem homomorfismos entre os respectivos anéis de faces induzido por inclusão de dois complexos simpliciais. Por exemplo, a inclusão natural do 1-esqueleto de um 2-simplexo não induz um homomorfismo dos anéis respectivos (vide Figura 3.2)

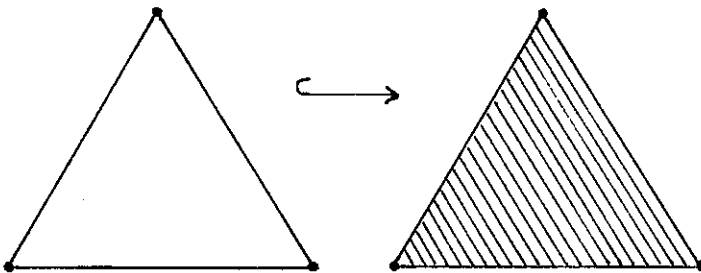


Fig. 3.2: O anel de Stanley-Reisner não é funtorial

Esta pode ser uma das razões pelas quais a transferência de  $k[\Delta]$  a  $\Delta$  é uma casca de noz, deficiência que nos obriga a aprofundar a combinatória de  $\Delta$  em termos de invariantes globais de  $k[\Delta]$ . A próxima seção procede neste sentido.

**3.7 Série de Hilbert e  $h$ -seqüências.** Se  $E$  é um espaço vetorial sobre  $k$ , denotaremos a sua dimensão por  $\dim_k E$  ou, simplesmente,  $\dim E$ , estando o corpo subentendido.

(3.7.1) DEFINIÇÃO. Seja  $\Delta$  um complexo simplicial. A *função de Hilbert* de  $k[\Delta]$  é

$$H(k[\Delta], -) : \mathbb{N} \longrightarrow \mathbb{N}, \quad m \mapsto \dim k[\Delta]_m,$$

onde  $k[\Delta]_m$  denota o subespaço vetorial de  $k[\Delta]$  cujos elementos são os resíduos dos polinômios homogêneos de grau  $m$ .

O cálculo explícito da função de Hilbert de  $k[\Delta]$  é extremamente simples, graças ao Lema (3.6.3).



(3.7.2) PROPOSIÇÃO. Para um complexo simplicial  $\Delta$  de dimensão  $d - 1$  ( $= \dim k[\Delta] - 1$ ), tem-se

$$H(k[\Delta], m) = \begin{cases} \sum_{i=0}^{d-1} f_i \binom{m-1}{i}, & m \geq 1 \\ 1, & m = 0 \end{cases}$$

onde  $f_i := \#\{F \in \Delta \mid \dim F = i\}$ .

(Lembramos que  $\binom{s}{r} = 0$  se  $s < r$ . É conveniente definir  $f_{-1} = 1$ , para efeito de uniformidade de certas expressões.)

DEMONSTRAÇÃO: De acordo com (3.6.3), uma base de  $k[\Delta]_m$  é dada pelos (resíduos dos) monômios cujos suportes são faces de  $\Delta$ . Assim, para cada face  $\{X_{l_1}, \dots, X_{l_{i+1}}\}$  fixa de dimensão  $i \leq m$ , devemos contar o número de monômios  $X_{l_1}^{r_1} \dots X_{l_{i+1}}^{r_{i+1}}$  de grau  $m$  tais que  $r_j \neq 0$ ,  $1 \leq j \leq i + 1$ . Ora, tal número é precisamente  $\binom{m-1}{i}$ , o que mostra a afirmação. ■

(3.7.3) DEFINIÇÃO. A *série de Hilbert* de  $k[\Delta]$  é a série formal

$$F(k[\Delta], z) := \sum_{m \geq 0} H(k[\Delta], m) z^m.$$

(3.7.4) COROLÁRIO.  $F(k[\Delta], z) = \sum_{i=-1}^{d-1} f_i z^{i+1} / (1 - z)^{i+1}$ .

DEMONSTRAÇÃO: Exercício. ■

À semelhança da teoria dos politopos, o vetor

$$f(\Delta) := (f_0, f_1, \dots, f_{d-1}), \quad \dim \Delta = d - 1,$$

é chamado o *f-vetor* de  $\Delta$ .

É natural perguntar se existe para complexos simpliciais uma teoria paralela à dos politopos, no que diz respeito às equações de Dehn-Sommerville (vide Capítulo 2, (2.4.15)). Ora, a demonstração lá baseou-se, fortemente, no teorema de Euler. Infelizmente, tal resultado só vale, em geral, para politopos.

Diante desta perplexidade, pode-se esperar algum outro resultado de tipo combinatório para *f*-vetores de complexos simpliciais? A resposta é afirmativa e é o conteúdo de um teorema notável de Katona e Kruskal, obtido independentemente.

Para enunciar este resultado, introduzimos expansões combinatórias de números inteiros, uma idéia que recua até Macaulay (pelo menos).

(3.7.5) PROPOSIÇÃO. *Dados inteiros positivos  $p, i$ , existe uma única sequência de inteiros  $n_i > n_{i-1} > \dots > n_j \geq j \geq 1$  tais que*

$$p = \binom{n_i}{i} + \binom{n_{i-1}}{i-1} + \dots + \binom{n_j}{j}.$$

DEMONSTRAÇÃO: Exercício. ■

Chamemos esta expansão de *desenvolvimento combinatório  $i$ -ádico* do inteiro  $p$ .

Utilizando a sequência dos inteiros  $n_i$  unicamente determinada, podemos definir também a  *$i$ -ésima pseudo-potência* de  $p$ , a saber

$$p^{(i)} = \binom{n_i}{i+1} + \binom{n_{i-1}}{i} + \dots + \binom{n_j}{j+1}$$

e a  *$i$ -ésima super-pseudo-potência* de  $p$ :

$$p^{(i)} = \binom{n_i+1}{i+1} + \binom{n_{i-1}+1}{i} + \dots + \binom{n_j+j}{j+1}.$$

(3.7.6) TEOREMA. [Kat66], [Kru63] *Um vetor  $(f_0, f_1, \dots, f_{d-1}) \in \mathbb{Z}^d$  é o  $f$ -vetor de um complexo simplicial de dimensão  $d-1$  se e somente se valem*

$$0 < f_{i+1} \leq f_i^{(i+1)}, \quad 0 \leq i \leq d-2.$$

O autor, honestamente, se inclui entre aqueles que citam o teorema de Katona–Kruskal, desconhecendo a demonstração do mesmo – o que não o impede, em absoluto, de apreciar seu conteúdo.

(3.7.7) EXERCÍCIO. Interprete a condição do Teorema (3.7.6) para  $i = 0$ , no caso de um complexo simplicial oriundo de um grafo (vide 2.5).

Gostaríamos de mencionar, explicitamente, o seguinte problema, cuja solução não parece ser tão óbvia.

(3.7.8) PROBLEMA. Descrever (ou refinar) as desigualdades de Katona–Kruskal para o caso de complexos simpliciais grafais.

A definição da função de Hilbert de um  $k[\Delta]$  se estende a um anel graduado qualquer  $A := k[\underline{X}]/I$ , da maneira óbvia, colocando-se  $H(A, m) :=$

$\dim_k A_m$ , onde  $A_m$  designa o subespaço de  $A$  gerado pelos resíduos dos polinômios de grau  $m$ .

Reportando ao teorema menor de Macaulay (3.3.3), observemos que ele fornece um critério para que uma função  $f : \mathbb{N} \rightarrow \mathbb{N}$  seja a função de Hilbert de um anel graduado  $A$  de tara  $(d_1, \dots, d_n)$ , a saber, é necessário e suficiente que exista um ideal de ordem  $\mathcal{J}$  do conjunto parcialmente ordenado dos termos do anel de polinômios de tara  $(d_1, \dots, d_n)$  tal que  $f(n) = \#\{M \in \mathcal{J} \mid \text{grau } M = n\}$ .

Com efeito, o teorema fornece a implicação mais difícil; para a outra, dado um ideal de ordem  $\mathcal{J}$  nestas condições, definimos  $A := k[\underline{X}]/I$ , onde  $I = (\mathfrak{M} \setminus \mathcal{J})$ .

Infelizmente, trata-se de um critério puramente existencial, de valor prático limitado. Esta deficiência, observada pelo próprio Macaulay, conduziu-o a um outro critério que testa um *único* subconjunto de  $\mathfrak{M}$ , algoritmicamente definido.

Por razões de sistematização, a seguinte noção foi popularizada por Stanley [Sta83], elaborando resultados de vários autores [Mac27], [Spe30], [Whi28], [CILi69].

(3.7.9) DEFINIÇÃO. Seja  $\mathcal{J} \subset \mathfrak{M}$  um ideal de ordem. Coloquemos  $h_i := \#\{M \in \mathcal{J} \mid \text{grau } M = i\}$ . A *h-sequência* de  $\mathcal{J}$  é a sequência  $h(\mathcal{J}) := (h_0, h_1, \dots)$ . Se a tara de  $k[\underline{X}]$  for  $(1, \dots, 1)$ , diremos que a *h-sequência* é *homogênea*.

A razão da notação de vetor, ao invés da de sequência infinita, é um hábito da teoria simplicial.

Finalmente, seja  $h : \mathbb{N} \rightarrow \mathbb{N}$  uma função arbitrária tal que  $h(0) = 1$ . Seja  $d := h(1)$ . Como em 3.3, fixemos a ordem lexicográfica reversa do semigrupo  $\mathfrak{M}$  de termos de  $k[X_1, \dots, X_d]$ . Suponhamos  $k[X_1, \dots, X_d]$  munido da tara  $(1, \dots, 1)$ . Para  $n \in \mathbb{N}$ , seja  $\mathfrak{H}_n$  a sequência dos  $n$  primeiros monômios de grau  $n$  de  $\mathfrak{M}$ . O conjunto

$$\mathfrak{H} := \bigcup_{n \geq 0} \mathfrak{H}_n \subset \mathfrak{M}$$

é a *sequência monomial léxica* da função  $h : \mathbb{N} \rightarrow \mathbb{N}$ .

Como apontamos mais acima, o teorema menor de Macaulay diz que uma função  $h : \mathbb{N} \rightarrow \mathbb{N}$  é a função de Hilbert de algum anel graduado se e só

se seus valores formam a  $h$ -sequência de algum ideal de ordem de termos. Restringindo a discussão a anéis graduados homogêneos, temos o seguinte resultado mais forte.

(3.7.10) TEOREMA. (Teorema maior de Macaulay) *As seguintes condições são equivalentes para uma função  $h : \mathbb{N} \rightarrow \mathbb{N}$ :*

- (i)  $h$  é a função de Hilbert de um anel graduado homogêneo.
- (ii)  $h(0) = 1$  e  $h(n+1) \leq h(n)^{\binom{n}{n}}$ , para todo  $n$ .
- (iii) A sequência monomial léxica de  $h$  é um ideal de ordem.

(3.7.11) EXERCÍCIO. Demonte a equivalência das condições (i) e (ii) de (3.7.10).

O mérito de Macaulay reside na demonstração da implicação (i)  $\Rightarrow$  (iii), para o que remetemos o leitor às referências acima citadas.

(3.7.12) EXERCÍCIO. ([Sta78]) Considere a função  $h : \mathbb{N} \rightarrow \mathbb{N}$  assim definida:

$$h(n) = \begin{cases} 1, & n = 0 \\ 3, & n = 1 \\ 4, & n = 2 \\ 5, & n = 3 \\ 7, & n = 4 \\ 0, & n \geq 5. \end{cases}$$

Mostre que não existe anel homogêneo admitindo  $h$  como função de Hilbert.

CAPITULO

**4**

ÁLGEBRA COMUTATIVA, II: O FATO  
COHEN-MACAULAY

## Capítulo 4. Álgebra Comutativa, II: O fato Cohen–Macaulay

### COHEN–MACAULAY, I

**4.1 Anéis de Cohen–Macaulay.** Para as noções básicas de álgebra comutativa, remetemos o leitor à *Terminologia*.

Seja  $A := k[\underline{X}]/I$  um anel graduado. A espinha dorsal deste capítulo é a seguinte noção.

(4.1.1) DEFINIÇÃO.  $A$  é um anel de *Cohen–Macaulay* se

$$\dim A = \text{prof}_{(\underline{X})} A.$$

Existem diversas caracterizações desta propriedade no contexto de álgebra comutativa e o especialista desta área, provavelmente, se sentiria privado de seus hábitos ao ler esta seção. Mas, o preço tem de ser pago em alguma parte, se quisermos aprofundar as propriedades numérico-combinatórias dos anéis de arestas e de faces.

Como gesto de conciliação, listamos a seguir algumas destas caracterizações.

(4.1.2) PROPOSIÇÃO. *As seguintes condições são equivalentes para um anel graduado  $A := k[\underline{X}]/I$ :*

- (i)  $A$  é um anel de *Cohen–Macaulay*.
- (ii)  $A$  admite um sistema de parâmetros que é uma  $A$ -sequência.
- (iii)  $A$  admite um sistema de parâmetros homogêneos que é uma  $A$ -sequência.
- (iv) Todo sistema de parâmetros de  $A$  contido em  $(\underline{X})$  é uma  $A$ -sequência.
- (v) Se  $\{\theta_1, \dots, \theta_d\} \subset (\underline{X})$  é um sistema de parâmetros de  $A$  e se  $\bar{A} := A/(\theta_1, \dots, \theta_d)$ , tem-se

$$F(A, z) = \frac{F(\bar{A}, z)}{\prod_{i=1}^d (1 - z^{e_i})},$$

onde  $e_i = \text{grau } \theta_i$ ,  $1 \leq i \leq d$ .

COMPLEMENTO. Se  $A$  é um anel graduado homogêneo (isto é, munido de tara  $(1, \dots, 1)$ ), os elementos  $\theta_1, \dots, \theta_d$  do sistema de parâmetros podem ser escolhidos de tal modo a serem todos de grau 1.

Chamamos a atenção do leitor, muito especialmente, para o item (v) da proposição, que relaciona a série de Hilbert (cf. 3.7) de  $A$  com a do anel  $\bar{A}$ , este último de dimensão zero, dito obtido de  $A$  mediante *redução por um sistema de parâmetros*.

(4.1.3) EXEMPLO. O anel de polinômios  $A = k[\underline{X}]$ , munido de tara arbitrária  $(d_1, \dots, d_n)$  é de Cohen–Macaulay: as variáveis  $\underline{X}$  formam uma  $A$ -sequência. Observemos que (v) fornece, neste caso, a seguinte expressão para a série de Hilbert de  $A$ :

$$F(A, z) = \frac{1}{\prod_{i=1}^n (1 - z^{d_i})}.$$

Esta expressão também poderia ter sido obtida diretamente da definição de  $F(A, z)$ .

(4.1.4) EXEMPLO. (Interseção completa) Se  $k[\underline{X}]$  é um anel de polinômios munido de tara  $(e_1, \dots, e_n)$  e se  $I$  é gerado por uma  $A$ -sequência  $\{f_1, \dots, f_m\} \subset \underline{X}$  tal que  $\text{grau } f_j = \delta_j$ , então  $A := k[\underline{X}]/I$  é um anel de Cohen–Macaulay e vale

$$F(A, z) = \frac{\prod_{j=1}^m (1 - z^{\delta_j})}{\prod_{i=1}^n (1 - z^{e_i})}.$$

A fórmula de redução da série de Hilbert para anéis de Cohen–Macaulay se generaliza para anéis quaisquer através da seguinte técnica.

Primeiramente, definimos a *função de Hilbert* de um ideal homogêneo  $J \subset A$ , onde  $A$  é um anel graduado (não necessariamente o anel  $k[\underline{X}]$ ):

$$H(J, m) := \dim_k J_m$$

onde  $J_m$  designa o  $k$ -espaço vetorial dos polinômios de peso  $m$ . Similarmente, definimos a série de Hilbert de  $J$ ,  $F(J, z) := \sum_{m \geq 0} H(J, m)z^m$ .

(4.1.5) LEMA. Seja  $A$  um anel graduado e seja  $\theta \in A$  um elemento de grau (= peso)  $\delta$ . Então vale:

$$F(A, z) = \frac{F(A/(\theta), z) - F((0 : \theta), z)z^\delta}{1 - z^\delta},$$

onde  $(0 : \theta) := \{a \in A \mid a\theta = 0\}$  (o anulador de  $\theta$ ).

DEMONSTRAÇÃO: Para qualquer ideal homogêneo  $J \subset A$ , tem-se, facilmente,  $H(A, m) = H(J, m) + H(A/J, m)$ . Em particular,  $H((\theta), m) = H(A, m) - H(A/(\theta), m)$ .

Por outro lado, a multiplicação por  $\theta$  em  $A_m$  é uma aplicação  $k$ -linear cujo núcleo é  $(0 : \theta)_m$  e cuja imagem é  $\theta A_m \subset A_{m+\delta}$ . Juntando estas informações, obtemos

$$\begin{aligned} H(A, m) &= \dim A_m = \dim \theta A_m + \dim(0 : \theta)_m \\ &= H((\theta), m) + H((0 : \theta), m) \\ &= H(A, m + \delta) - H(A/(\theta), m + \delta) + H((0 : \theta), m). \end{aligned}$$

Passando às séries de Hilbert, resulta

$$\begin{aligned} F(A, z) - F((0 : \theta), z) &= \frac{F((\theta), z)}{z^\delta} \\ &= \frac{F(A, z) - F(A/(\theta), z)}{z^\delta}, \end{aligned}$$

como queríamos. ■

(4.1.6) COROLÁRIO. Se  $A$  é graduado e  $\theta_1, \dots, \theta_r$  é uma  $A$ -sequência de elementos homogêneos, tem-se

$$F(A, z) = \frac{F(\overline{A}, z)}{\prod_{j=1}^r (1 - z^{\delta_j})},$$

onde  $\delta_j = \text{grau } \theta_j$  e  $\overline{A} = A/(\theta_1, \dots, \theta_r)$ .

DEMONSTRAÇÃO: Basta observar que se  $\theta$  não é divisor de zero, então  $(0 : \theta) = (0)$ . O resto segue do lema acima, por indução sobre  $r$ . ■

Elaborando o teorema maior de macaulay, Stanley obteve um critério para que uma função aritmética seja a função de Hilbert de um anel graduado *homogêneo* com profundidade prescrita, em termos das  $h$ -sequências (cf. 3.7).



(4.1.7) TEOREMA. ([Sta78] Seja  $h : \mathbf{N} \rightarrow \mathbf{N}$  uma função arbitrária e  $r \geq 0$  um inteiro. As seguintes condições são equivalentes:

(i)  $h$  é a função de Hilbert de algum anel graduado homogêneo tal que  $\text{prof}_{(X)} A \geq r$ .

(ii) Se

$$\sum_{i=0}^{\infty} h_{i,r} z^i := (1-z)^r \sum_{m=0}^{\infty} h(m) z^m,$$

então  $(h_{0,r}, h_{1,r}, \dots)$  é uma  $h$ -sequência.

DEMONSTRAÇÃO: (i)  $\Rightarrow$  (ii) De acordo com o teorema de normalização (cf. *Terminologia*),  $A$  admite um sub-sistema de parâmetros  $\theta_1, \dots, \theta_r$  que é uma  $A$ -sequência, com grau  $\theta_i = 1$ , para todo  $i$ . Por (4.1.6), aplicado nesta situação, obtém-se

$$(1-z)^r \sum_{m \geq 0} h(m) z^m = (1-z)^r F(A, z) = F(A/(\theta_1, \dots, \theta_r), z).$$

Logo, pelo teorema maior de Macaulay,  $(h_{0,r}, h_{1,r}, \dots)$  é uma  $h$ -sequência.

(ii)  $\Rightarrow$  (i) Pelo teorema maior de Macaulay, existe um anel graduado  $B$  tal que  $H(B, i) = h_{i,r}$ , para todo  $i \geq 0$ . Seja  $A := B[Y_1, \dots, Y_r]$  o anel de polinômios em  $r$  indeterminadas, a coeficientes em  $B$ . Com grau  $Y_i = 1$ ,  $A$  é um anel homogêneo. Evidentemente,  $Y_1, \dots, Y_r$  é uma  $A$ -sequência; logo  $\text{prof } A \geq r$ . A conclusão vem de observar as igualdades

$$\begin{aligned} \sum_{m \geq 0} h(m) z^m &= \frac{\sum_{i \geq 0} h_{i,r} z^i}{(1-z)^r} = \frac{\sum_{i \geq 0} H(B, i) z^i}{(1-z)^r} \\ &= \frac{F(B, z)}{(1-z)^r} = F(A, z), \end{aligned}$$

a última das quais segue de (4.1.6). ■

(4.1.8) EXERCÍCIO. Mostre que uma função  $h : \mathbf{N} \rightarrow \mathbf{N}$  é a função de Hilbert de um anel graduado homogêneo de Cohen–Macaulay, de dimensão  $d$ , se e somente se a série formal  $(1-z)^d \sum_{m \geq 0} h(m) z^m$  é um polinômio e os coeficientes deste formam uma  $h$ -sequência.

(*Sugestão*: Usar (4.1.7), lembrando que a redução por um sistema de parâmetros tem dimensão zero; em seguida, usar o teorema maior de Macaulay, pelo qual  $h$ -sequências homogêneas e sequências monomiais léxicas são equivalentes.)

(4.1.9) EXERCÍCIO. Seja  $A$  um dos seguintes anéis:

(i)  $k[X, Y]/(X^2, XY)$ ;

(ii)  $k[X, Y, Z]/(XY, XZ)$ ;

(iii)  $k[X, Y, Z]/(XY, XZ, YZ)$ .

Determine, em cada um destes casos,  $\dim A$  e  $F(A, z)$  e decida se  $A$  é ou não um anel de Cohen–Macaulay.

Após este *intermezzo* abstrato, é tempo de voltar às aplicações à teoria simplicial.

Primeiramente, reformemos a série de Hilbert simplicial, obtida na Proposição (3.7.4), nos moldes dos resultados desta seção. Seja  $A := k[\Delta] = k[\underline{X}]/I_\Delta$  o anel das faces de um complexo simplicial  $\Delta$ . Neste caso, tem-se

$$(4.1-1) \quad (1 - z)^d F(A, z) = f_{-1}(1 - z)^d + f_0 z(1 - z)^{d-1} + \dots + f_{d-1} z^d$$

onde  $d = \dim \Delta + 1$ . Desenvolvendo o segundo membro de (4.1-1), obtém-se um polinômio de grau  $d$ , cujos coeficientes são

$$(4.1-2) \quad h_j := \sum_{i=0}^j (-1)^{j-1} \binom{d-i}{j-i} f_{i-1}, \quad 0 \leq j \leq d.$$

O vetor  $h(\Delta) := (h_0, h_1, \dots, h_d)$  é remanescente das  $h$ -sequências e é, por tal, chamado de  $h$ -vetor de  $\Delta$ .

Na verdade, existe mais do que uma reminiscência, como revela o resultado a seguir.

(4.1.10) DEFINIÇÃO. Um complexo simplicial  $\Delta$  é dito ser de *Cohen–Macaulay* se o anel  $k[\Delta]$  é de Cohen–Macaulay.

(4.1.11) PROPOSIÇÃO. Se  $\Delta$  é um complexo simplicial de Cohen–Macaulay, então o  $h$ -vetor de  $\Delta$  é uma  $h$ -sequência.

DEMONSTRAÇÃO: Resulta, imediatamente, do critério (4.1.7). ■

Em geral, se  $\text{prof } k[\Delta] = r \leq d = \dim k[\Delta]$ , tem-se, sempre por (4.1.7), que os coeficientes da série

$$(1-z)^r F(k[\Delta], z) = \frac{f_{-1}(1-z)^d + f_0 z(1-z)^{d-1} + \dots + f_{d-1} z^d}{(1-z)^{d-r}}$$

formam uma  $h$ -sequência (infinita), ao passo que o  $h$ -vetor (sempre finito) pode ter, inclusive, coeficientes negativos!

(4.1.12) EXEMPLO. O complexo simplicial cuja realização poliédrica é mostrada na Figura 4.1, tem  $f$ -vetor  $(5, 6, 2)$ . Pelas fórmulas (4.1-2),  $h_2 = -1$ . Consequentemente, o complexo não é de Cohen-Macaulay.

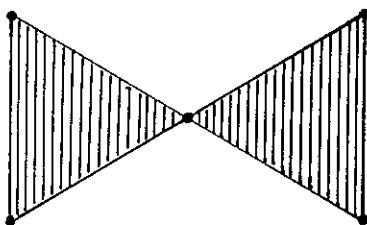


Fig. 4.1: Um complexo simplicial que não é de Cohen-Macaulay

A razão por trás deste “mau” comportamento é a não construtibilidade do complexo simplicial da Figura 4.1, segundo Hochster.

(4.1.13) DEFINIÇÃO. Seja  $\mathfrak{P} \subset \mathbb{R}^m$  um politopo e seja

$$\partial\mathfrak{P} := \bigcup_{F \subset \mathfrak{P}} F, \quad F \text{ faceta,}$$

a sua *fronteira*. Considere-se o reticulado  $\mathcal{L}(\mathfrak{P})$  dos subconjuntos de  $\partial\mathfrak{P}$  que são reuniões de faces. A família  $\mathcal{L}_c(\mathfrak{P})$  dos subconjuntos *construtíveis* de  $\mathcal{L}(\mathfrak{P})$  é definida, recursivamente, pelas seguintes exigências:

- (1) Se  $F \subset \mathfrak{P}$  é uma face, então  $F \in \mathcal{L}_c(\mathfrak{P})$ ;
- (2) Se  $B_1, B_2, B_1 \cap B_2$  pertencem todos a  $\mathcal{L}_c(\mathfrak{P})$  e se  $\dim B_1 = \dim B_2 = \dim B_1 \cap B_2 + 1$ , então  $B_1 \cup B_2$  também pertence a  $\mathcal{L}_c(\mathfrak{P})$ .

Para enunciar o próximo resultado, observamos que todo conjunto  $B \in \mathcal{L}(\mathfrak{P})$  é a realização poliédrica de um sub-complexo simplicial  $\Delta_B$  do complexo simplicial abstrato das faces do politopo  $\mathfrak{P}$ .

(4.1.14) PROPOSIÇÃO. ([Hoc72]) *Seja  $\mathfrak{P}$  um politopo e seja  $B \in \mathcal{L}_c(\mathfrak{P})$ . Então o complexo simplicial  $\Delta_B$  é de Cohen–Macaulay.*

DEMONSTRAÇÃO: (Esboço) Queremos mostrar que o anel de faces  $k[\Delta_B]$  é de Cohen–Macaulay. Como  $\Delta_B$  é construtível, ele é obtido pelo processo recursivo montado em (4.1.13). O problema se reduz, então, ao seguinte problema da teoria dos anéis: dados ideais homogêneos  $I, J \subset A := k[\underline{X}]$  tais que  $A/I$  e  $A/J$  são anéis de Cohen–Macaulay de dimensão  $d$  e  $A/(I+J)$  é também de Cohen–Macaulay, de dimensão  $d - 1$ , então  $A/I \cap J$  é de Cohen–Macaulay.

A demonstração do último fato é a principal observação de Hochster. Resulta de uma *sequência exata* natural de homomorfismos

$$\begin{aligned} 0 \longrightarrow A/I \cap J \longrightarrow A/I \oplus A/J \longrightarrow A/(I+J) \longrightarrow 0 \\ \bar{a} \mapsto (\bar{a}, \bar{a}) \\ (\bar{a}_1, \bar{a}_2) \mapsto \bar{a}_1 + \bar{a}_2 \end{aligned}$$

e do comportamento da profundidade ao longo de tais sequências. Remetemos o leitor à *Terminologia*, onde encontrará os pre-requisitos para formular, rigorosamente, o argumento acima. ■

(4.1.15) EXEMPLO. ([BrMa71]) *A fronteira de um politopo é sempre construtível.*

(4.1.16) OBSERVAÇÃO. Stanley considerou a noção de construtibilidade de complexos simpliciais abstratos. Nesta formulação, o complexo de cadeias da estrutura subjacente de um reticulado distributivo é construtível. Conforme foi mencionado em (1.6.1)(iii), um reticulado distributivo é, a menos de isomorfismos ordenados, um transformado de ideais de ordem de um conjunto parcialmente ordenado. Infelizmente, conjuntos parcialmente ordenados de grande interesse, tais como o das coberturas de vértices de um grafo, não admitem estrutura automática de reticulado.

Complexos de cadeias surgem, como complexos simpliciais de Cohen–Macaulay, em outros contextos que não o da construtibilidade. Um dos resultados deste tipo é devido a Baclawski e Garsia, que se basearam fortemente na decomposição de Hironaka–Rees da seção 3.4.

(4.1.17) TEOREMA. ([BaGa81]) *Seja  $\Delta$  um complexo simplicial e seja  $\Delta_c := \Delta_c(\Delta)$  o complexo das cadeias do conjunto parcialmente ordenado*

subjacente a  $\Delta$ . Se  $\Delta_c$  é de Cohen–Macaulay então  $\Delta$  é de Cohen–Macaulay.

DEMONSTRAÇÃO: (Esboço) A demonstração usa uma técnica de retificação no espírito do que foi exposto nas seções 3.2, 3.3 e 3.4. Daremos apenas os elementos principais da argumentação.

A primeira etapa consiste em mostrar que os anéis respectivos,  $k[\Delta_c]$  e  $k[\Delta]$ , são isomorfos como  $k$ -espaços vetoriais (mas, atenção: os dois não são isomorfos como anéis, com se vê, facilmente, mediante exemplos). Na verdade, temos um isomorfismo privilegiado

$$\varphi : k[\Delta_c] \longrightarrow k[\Delta]$$

definido usando as bases respectivas de monômios cujos suportes são faces do complexo simplicial.

No caso do complexo simplicial  $\Delta_c$ , os monômios básicos estão associados a multicadeias (vide 1.6) cujos suportes são faces de  $\Delta_c$ . Uma tal multicadeia pode, então, ser apresentada sob a forma

$$X_{\sigma_1} \cdots X_{\sigma_m}, \quad \sigma_i \in \Delta, \quad \sigma_1 \leq \cdots \leq \sigma_m.$$

Por outro lado, para o mesmo elemento  $\sigma_1 \leq \cdots \leq \sigma_m$ , temos que o monômio

$$X^{\sigma_1} \cdots X^{\sigma_m}, \quad X^{\sigma_i} := \prod_{v \in \sigma_i} X_v,$$

tem por suporte a face  $\sigma_m \in \Delta$ .

Definimos, então,  $\varphi(X_{\sigma_1} \cdots X_{\sigma_m}) = X^{\sigma_1} \cdots X^{\sigma_m}$ .

Deixamos ao leitor a tarefa de verificar que  $\varphi$  admite uma inversa  $k$ -linear (que, aplicada a um monômio básico de  $k[\Delta]$ , fornece a chamada *fatoração básica* (“standard”) deste monômio).

A segunda etapa, mais delicada, consiste na técnica de retificação propriamente dita. Alguns dos preliminares se assemelham aos do caso determinantal mencionado mais acima. Usamos a noção de vetor de multiposto de um monômio básico  $X_{\sigma_1} \cdots X_{\sigma_m}$  de  $k[\Delta_c]$  (vide 1.6), com a imposição adicional de que o vetor satisfaça a condição  $\#\sigma_1 \leq \cdots \leq \#\sigma_m$ : neste caso, dizemos que o multiposto é a *fôrma* do monômio  $X_{\sigma_1} \cdots X_{\sigma_m}$ .

Em seguida, ordenamos as fôrmas dos monômios básicos de  $k[\Delta_c]$  mediante a ordem lexicográfica:

$$(\sigma_1, \dots, \sigma_m) \geq (\tau_1, \dots, \tau_l)$$

se e só se ou  $m < l$  ou  $m = l$  e  $\sigma_1 = \tau_1, \dots, \sigma_{i-1} = \tau_{i-1}, \sigma_i > \tau_i$ , para algum  $i$ . Usando a fatoração básica para os monômios de  $k[\Delta]$ , temos uma noção análoga de fôrma para estes monômios.

O peso da demonstração consiste na seguinte afirmação: *dados elementos  $f_1, \dots, f_m$  em  $k[\Delta_c]$ , a diferença  $\varphi(f_1 \cdots f_m) - \varphi(f_1) \cdots \varphi(f_m)$  é (não nula, mas) uma combinação  $k$ -linear de monômios cujas fôrmas precedem, estritamente, a fôrma obtida por reunião disjunta (totalmente ordenada) das fôrmas dos monômios que ocorrem em  $f_1, \dots, f_m$ .*

Uma vez demonstrada esta afirmação, resta a terceira etapa, que consiste, a grosso modo, em aplicar o isomorfismo  $\varphi$  à decomposição de Hironaka-Rees do anel  $k[\Delta_c]$  (que é de Cohen-Macaulay, por hipótese).

Isto fecha o esboço da demonstração. ■

(4.1.18) EXERCÍCIO. Considere o complexo simplicial das faces de um 2-simplexo.

- (i) Mostre que  $\Delta_c(\Delta)$  admite, como realização geométrica, a divisão bari-cêntrica de  $\Delta$ .
- (ii) Mostre que  $\Delta_c(\Delta)$  é, de fato, grafal, exibindo o grafo correspondente.
- (iii) Mostre que os resíduos dos polinômios

$$X_1 + X_2 + X_3, \quad X_1X_2 + X_1X_3 + X_2X_3, \quad X_1X_2X_3$$

constituem um sistema de parâmetros de  $k[\Delta]$  e obtenha um sistema de parâmetros de  $k[\Delta_c]$ .

(Sugestão: primeiro, a dimensão de  $k[\Delta_c]$ ).

(4.1.19) EXERCÍCIO. Porque a demonstração de Baclawski-Garsia não implica na recíproca do Teorema (4.1.17)?

(4.1.20) EXERCÍCIO. Mostre que os resíduos dos polinômios

$$\theta_i := \sum_{\substack{\sigma \in \Delta \\ \#\sigma=i}} X^\sigma, \quad i = 0, 1, \dots$$

formam um sistema de parâmetros de  $k[\Delta]$ , onde, como acima,  $X^\sigma := \prod_{v \in \sigma} X_v$ .

**4.2 O teorema de Hochster–Munkres–Reisner.** O problema central da teoria dos complexos simpliciais abstratos é encontrar uma caracterização combinatória dos complexos simpliciais de Cohen–Macaulay. Na ausência desta, também seria satisfatório encontrar uma caracterização em termos do anel de Stanley Reisner, mais precisamente, dos invariantes típicos da teoria dos anéis.

O melhor resultado, até o momento, é uma caracterização homológica que, como bonus, mostra que a propriedade de Cohen–Macaulay para complexos simpliciais é topológica.

A ferramenta básica é constituída pela *homologia simplicial*, que mede, informalmente falando, o fracasso dos *ciclos* formados de cadeias de faces em serem fronteiras de tais cadeias de uma dimensão a mais.

Vejamos as noções básicas desta teoria, sem qualquer pretensão à completude. Para maiores detalhes, remetemos à bibliografia.

Seja, como antes,  $\Delta$ , um complexo simplicial de dimensão  $d$ . Sejam  $v_1, \dots, v_n$  os vértices de  $\Delta$ . Por  $C_i = C_i(\Delta)$  denotaremos o  $k$ -espaço vetorial com base o conjunto das  $i$ -faces de  $\Delta$  ( $-1 \leq i \leq d$ ). Um elemento deste espaço é chamado uma  *$i$ -cadeia*. Dada uma face  $F = \{v_{i_0}, \dots, v_{i_r}\} \in \Delta$ , com  $i_0 < i_1 < \dots < i_r$ , pomos  $F_j := F \setminus v_{i_j}$ . O *operador de bordo de ordem  $r$*  ( $r = 0, 1, \dots, d$ ) é a aplicação  $k$ -linear  $\partial_r : C_r \rightarrow C_{r-1}$  definida, nos elementos da base acima, pela seguinte expressão:

$$\partial_r(F) := \sum_{j=0}^r (-1)^j F_j.$$

Por conveniência, definimos  $\partial_{d+1} = 0$ .

Verifica-se que  $\text{Im } \partial_{r+1} \subseteq \text{Nuc } \partial_r$ .

(4.2.1) DEFINIÇÃO. A *homologia reduzida de ordem  $r$*  (a coeficientes em  $k$ ) de  $\Delta$  é o espaço vetorial quociente

$$\tilde{H}_r(\Delta, k) := \text{Nuc } \partial_r / \text{Im } \partial_{r+1}.$$

(4.2.2) EXERCÍCIO. (i) Mostre que  $\partial_r \partial_{r+1} = 0$ , para  $r = 0, 1, \dots, d$ .

(ii) Mostre que, como espaço vetorial,  $C_i(\Delta)$  é isomorfo ao subespaço de

$k[\Delta]_i$  gerado pelos monômios livres de quadrados (lembrar que, de acordo com (3.7.3), uma base para  $k[\Delta]_i$  é constituída por todos os monômios de grau  $i$  cujos suportes são faces de  $\Delta$ ).

(4.2.3) EXERCÍCIO. Mostre que se  $\Delta \neq \emptyset$ , então

$$\dim_k \tilde{H}_0(\Delta, k) = \kappa(\Delta) - 1$$

onde  $\kappa(\Delta)$  designa o número de componentes conexas de  $\Delta$ .

A homologia simplicial depende apenas da estrutura combinatória de  $\Delta$ . No outro extremo do espectro, existem várias teorias de homologia para espaços topológicos, por um lado, e cohomologias para anéis, por outro.

O teorema central desta seção admite três versões, uma para cada contexto homológico:

- (1) Homologia simplicial (Reisner);
- (2) Homologia singular (Munkres);
- (3) Cohomologia local (Hochster–Stanley).

Enquanto (1) tem seu contexto natural neste curso, (2) cabe num curso de topologia e (3) faz parte dos métodos homológicos de álgebra comutativa e geometria algébrica.

A homologia singular (reduzida) de ordem  $r$  (a coeficientes em  $k$ ) de um espaço topológico  $E$  e a sua versão relativa (não reduzida) para um subespaço  $E'$ , serão respectivamente denotadas por

$$\tilde{\mathcal{H}}_r(E, k) \quad \text{e} \quad \mathcal{H}_r(E, E', k).$$

A cohomologia local de ordem  $r$  (relativa ao ideal máximo  $(\underline{X})$ ) de um  $k[\underline{X}]$ -módulo graduado  $M$  será denotada

$$\mathcal{H}^r(M).$$

Dois resultados homológicos são básicos para o teorema. Devido à simplicidade dos respectivos enunciados – transparentes, mesmo sem o conhecimento do mecanismo destas teorias – serão incluídos aqui.

(4.2.4) PROPOSIÇÃO. *Seja  $\Delta$  um complexo simplicial e seja  $E_\Delta \subset \mathbb{R}^n$  uma realização poliédrica de  $\Delta$  (cf. 2.4). Então*

$$\tilde{H}_r(\Delta, k) \simeq \tilde{\mathcal{H}}_r(E_\Delta, k)$$



como espaços vetoriais, para todo  $r \geq 0$ .

(4.2.5) PROPOSIÇÃO. Seja  $I \subset k[\underline{X}]$  um ideal homogêneo e seja  $A := k[\underline{X}]/I$ . Então tem-se

$$\mathcal{H}^r(A) = 0, \quad \text{para } r < \text{prof } A \quad \text{e} \quad r > \dim A.$$

Em particular,  $A$  é um anel de Cohen–Macaulay se e só se

$$\mathcal{H}^r(A) = 0, \quad \text{para todo } r \neq \dim A.$$

Para entender a versão cohomológica de Hochster–Stanley, é conveniente munir  $k[\underline{X}]$  de uma graduação mais fina, usando  $\mathbb{N}^n$  no lugar de  $\mathbb{N}$ . Para tal, colocamos grau  $X_i = e_i$ , onde  $e_i$  designa o  $i$ -ésimo vetor coordenado canônico de  $\mathbb{N}^n$ . Temos, de maneira análoga às graduações usuais:

$$k[\underline{X}] = \sum_{\underline{d}} k[\underline{X}]_{\underline{d}}, \quad \underline{d} \in \mathbb{N}^n.$$

Esta graduação induz uma graduação do anel  $k[\Delta]$ , denominada *fina*. Em correspondência, definimos a *série de Hilbert fina*

$$F(k[\Delta], \underline{z}) = \sum_{\underline{d}} (\dim_k k[\Delta]_{\underline{d}}) \underline{z}^{\underline{d}}, \quad \underline{z} \in \mathbb{Z}[z_1, \dots, z_n].$$

De modo que estamos, agora, no domínio das séries formais a várias variáveis! Observamos que a cohomologia local  $\mathcal{H}^r(k[\Delta])$  herda também uma graduação fina, só que com respeito a  $\mathbb{Z}^n$  (e não  $\mathbb{N}^n$ ) – este fato não é óbvio, principalmente diante da nossa precária situação, sem as definições!

Mas, há outra obstrução mais séria: a cohomologia local, salvo em situações especiais, não é finitamente gerada. Isto obriga, enfim, a um grande *tour de force*, com séries de Laurent a várias variáveis e outros ingredientes menos palatáveis.

É de surpreender que, diante de tais dificuldades técnicas para ajustar os preliminares da teoria, possamos ter uma condição numérica razoável que caracterize a propriedade de Cohen–Macaulay para  $k[\Delta]$ .

Mas, aí vai.

(4.2.6) TEOREMA. ([Rei76], [Mun84], [Sta83]) Seja  $\Delta$  um complexo simplicial de dimensão  $d - 1$  e seja  $E_\Delta$  uma realização poliédrica de  $\Delta$ . As seguintes condições são equivalentes:

(i)  $k[\Delta]$  é um anel de Cohen–Macaulay.

(ii) (Reisner) Para toda  $F \in \Delta$  e para todo  $i < \dim el_\Delta F$ , tem-se

$$\tilde{H}_i(el_\Delta F) = 0.$$

(iii) (Munkres) Para todo  $p \in E_\Delta$  e para todo  $i < \dim E_\Delta$ , tem-se

$$\tilde{\mathcal{H}}_i(E_\Delta, k) \simeq \mathcal{H}_i(E_\Delta, E_\Delta \setminus \{p\}, k).$$

(iv) (Hochster–Stanley) Tem-se

$$F(\mathcal{H}^i(k[\Delta]), \underline{z}) = \sum_{F \in \Delta} \dim_k \tilde{H}_{d-1-|F|}(el_\Delta F, k) \prod_{x_i \in F} \frac{z_i^{-1}}{1 - z_i^{-1}},$$

onde  $|F| = \#F$ .

A demonstração de qualquer das equivalências do teorema está muito além dos objetivos do curso e é extremamente difícil. O teorema é considerado “duro” mesmo pelos especialistas. Isto não impede, contudo, que se possa apreciar seu funcionamento num caso particular simples.

(4.2.7) EXEMPLO. Considere o complexo simplicial  $\Delta$  com realização poliédrica indicada na Figura 4.1. Pelo critério do  $h$ -vetor, já sabemos que  $\Delta$  não é de Cohen–Macaulay (cf. 4.1.12). Mas, isto também segue do teorema acima, da seguinte maneira: considere-se o vértice  $v$  que conecta os dois simplexes de  $\Delta$ . O elo de  $v$  é a reunião de duas arestas disjuntas, logo  $\dim \tilde{H}_0(el_\Delta v, k) = 1$  (por (4.2.3)), o que contraria a condição (ii) de Reisner no teorema.

Uma aplicação interessante do teorema é a recíproca do teorema de Baclawski–Garsia (4.1.17), observada pelos próprios autores.

(4.2.8) TEOREMA. Seja  $\Delta$  um complexo simplicial e  $\Delta_c$  o complexo simplicial das cadeias correspondente. Se  $\Delta$  é de Cohen–Macaulay, então  $\Delta_c$  também o é.

DEMONSTRAÇÃO: (Esboço) O argumento procede, de modo elegante, ao longo das seguintes etapas:

- (1) (Junção) Dados dois complexos simpliciais  $\Delta_1$  e  $\Delta_2$ , com conjuntos de vértices disjuntos, a *junção* de  $\Delta_1$  e  $\Delta_2$  é o complexo simplicial

$$\Delta_1 * \Delta_2 := \{F_1 \cup F_2 \mid F_1 \in \Delta_1, F_2 \in \Delta_2\}.$$

- (2) (Bouquês) Um complexo simplicial  $\Delta$  é um *bouquê* se  $\tilde{H}_i(\Delta, k) = 0$ , para todo  $i < \dim \Delta - 1$ .
- (3) (Fórmula de Künneth) Se  $\Delta_1$  e  $\Delta_2$  são bouquês então  $\Delta_1 * \Delta_2$  é um bouquê.
- (4) Adicionemos ao conjunto parcialmente ordenado subjacente a  $\Delta$  um elemento mínimo  $\hat{0}$  e um elemento máximo  $\hat{1}$ . O complexo simplicial

$$el_{\Delta_c}(F_1 \subset \dots \subset F_k),$$

com  $F_1 \subset \dots \subset F_k$  uma cadeia de faces, é simplicialmente equivalente (vide 2.4) à junção

$$\Delta(\hat{0}, F_1) * \Delta(F_1, F_2) * \dots * \Delta(F_k, \hat{1}),$$

onde  $(F_i, F_{i+1})$  designa o *intervalo* de  $F_i$  a  $F_{i+1}$ .

- (5) Cada um dos intervalos  $(F_i, F_{i+1})$  é, por sua vez, um bouquê (incluindo  $(\hat{0}, F_1)$  e  $(F_k, \hat{1})$ ).

Admitindo-se estas etapas, o teorema segue imediatamente do teorema (4.2.6) (ii). Quanto às etapas propriamente ditas, (3) e (5) são as mais delicadas. A primeira é um formalismo de homologia geral; a segunda resulta de que os intervalos acima são *triangulações da esfera*, um assunto de topologia. ■

**4.3 A conjectura da cota superior.** Para motivar o principal resultado desta seção, devido a Stanley, reportemo-nos, por alguns instantes, à seção 2.4, onde foi definido o politopo cíclico  $C(n, d)$ .

Vimos (cf. (2.4.9)) que, para  $1 \leq k \leq \frac{d}{2}$ ,  $C(n, d)$  tem o maior número possível de  $(k - 1)$ -faces entre todos os  $d$ -politopos. Em 1957, Motzkin [Mot57] conjecturou que  $C(n, d)$  teria esta propriedade para *todo* valor de  $k$  no intervalo  $1 \leq k \leq d$ , isto é, que valeria, para qualquer  $d$ -politopo  $\mathfrak{P}$ , a cota

$$f(\mathfrak{P}) \leq f(C(n, d)).$$

Esta conjectura ficou sendo conhecida como a *Conjectura da Cota Superior*. Em 1970, McMullen [McM70] provou a conjectura de Motzkin.

(4.3.1) EXERCÍCIO. Para  $k > \frac{d}{2}$ , o valor  $f_{k-1}(C(n, d))$  não é mais o número combinatório  $\binom{n}{k}$ . Pode imaginar qual é este valor?

(Sugestão: Consultar as referências [Gr67], [McSh71]).

A demonstração da conjectura da cota superior procede, primeiramente, em relação aos polítopos simpliciais (vide 2.4), os quais têm o  $f$ -vetor maior possível entre todos os polítopos. Isto levantou a questão da validade da conjectura análoga para complexos simpliciais abstratos.

Para examinar de perto esta questão, reformulemos a conjectura em termos do  $h$ -vetor de um complexo  $\Delta$  — lembrando que, por definição, é o  $h$ -vetor do anel das faces  $k[\Delta]$ . Relendo as equações de Dehn–Sommerville (2.4.13) em termos do  $h$ -vetor de um  $d$ -polítopo  $\mathfrak{P}$ , definido, formalmente, pelas equações que relacionam as  $f$ -coordenadas e as  $h$ -coordenadas no caso de  $\Delta$  ((4.1-2)), obtemos

(4.3.2) PROPOSIÇÃO. (Dualidade de Dehn–Sommerville) Para um  $d$ -polítopo  $\mathfrak{P}$ , vale

$$(4.3-1) \quad h_i(\mathfrak{P}) = h_{d-i}(\mathfrak{P}), \quad 0 \leq i \leq \frac{d}{2}.$$

Em geral, um complexo abstrato  $\Delta$  satisfazendo (4.3-1) em relação ao seu  $h$ -vetor, será dito um *complexo de Dehn–Sommerville*.

(4.3.3) EXERCÍCIO. (i) Se  $\Delta$  é um complexo simplicial, escreva as coordenadas de  $\Delta$  em função de suas  $f$ -coordenadas (isto é, inverta as relações (4.1-2)).

(ii) Se  $\Delta$  e  $\Delta'$  são complexos simpliciais, mostre que  $f(\Delta) \leq f(\Delta')$  implica em  $h(\Delta) \leq h(\Delta')$ .

(4.3.4) PROPOSIÇÃO. Seja  $\Delta$  um complexo de Dehn–Sommerville com  $n$  vértices. Então são equivalentes: (i)  $h(\Delta) \leq h(C(n, d))$ .

(ii)  $h_i(\Delta) \leq \binom{n-d+i-1}{i}$ , para  $0 \leq i \leq \frac{d}{2}$ .

DEMONSTRAÇÃO: [Grü67]. ■

Mediante (4.3.2) e (4.3.3), temos a seguinte formulação:

(4.3.5) CONJETURA. (Cota Superior, CS) Se  $\Delta$  é um complexo abstrato com  $n$  vértices, vale

$$h(\Delta) \leq h(C(n, d)).$$

(Cota Superior Condicionada, CSC) Se  $\Delta$  é um complexo com  $n$  vértices, vale

$$h_i(\Delta) \leq \binom{n-d+i-1}{i}, \quad \text{para } 0 \leq i \leq \frac{d}{2}.$$

De posse da teoria desenvolvida em 3.7 e 4.1, estamos em condições de (enunciar e) provar o teorema de Stanley.

(4.3.6) TEOREMA. ([Sta83]) Se  $\Delta$  é um complexo simplicial de Cohen-Macaulay, então CSC é verdadeira.

DEMONSTRAÇÃO: Por (4.1-2), temos, facilmente,  $h_1(\Delta) = n - d$ , onde  $n$  é o número de vértices de  $\Delta$  e  $d = \dim k[\Delta]$ . Pelo teorema maior de Macaulay (3.7.10), o  $h$ -vetor de  $\Delta$  é uma  $h$ -sequência homogênea, logo  $h_i(\Delta)$  não pode exceder o número total de monômios de grau  $i$  em  $n - d$  variáveis, que é o número combinatório da conjectura. ■

(4.3.7) COROLÁRIO. Seja  $\Delta$  um complexo cuja realização poliédrica é topologicamente equivalente a um dos seguintes espaços:

- (1) Uma esfera  $S^{d-1} \subset \mathbb{R}^d$ .
- (2) A fronteira  $\partial\mathfrak{B}$  de um  $d$ -politopo simplicial.

Então, CS é verdadeira para  $\Delta$ .

DEMONSTRAÇÃO: Em ambos os casos,  $\Delta$  é de Dehn-Sommerville – vide [Kle64] para o caso de (1) e [Grü67], para o caso (2). Por outro lado, em ambos os casos,  $\Delta$  satisfaz as condições do Teorema 4.2.6 (no caso de (2), vide também 4.1.15). Consequentemente,  $\Delta$  é de Cohen-Macaulay e o resultado segue de (4.3.6). ■

(4.3.8) OBSERVAÇÃO. Se  $\Delta$  é de Dehn-Sommerville, então a cotá da CSC é redundante no intervalo  $\frac{d}{2} \leq i \leq d - 1$ . Se  $\Delta$  é de Cohen-Macaulay, mas não de Dehn-Sommerville, as estimativas neste intervalo não são redundantes. Põe-se a questão de saber que tipo de dualidade à la Dehn-Sommerville subsiste, em geral.

Esta questão relaciona-se com a chamada *conjectura da cota inferior*, originalmente enunciada por McMullen para o caso de politopos simpliciais e resolvida, neste caso, por Billera-Lee e Stanley. Esta conjectura tem uma contra-partida em álgebra comutativa ligada à noção de anel de Gorenstein, que é um anel de Cohen-Macaulay gozando de um tipo de dualidade.

Considerações desta natureza nos levariam muito além dos nossos objetivos, razão pela qual sugerimos a consulta à bibliografia ([Sta78], por exemplo).

## COHEN-MACAULAY, II

**4.4 A suspensão de um grafo.** A partir de agora e até o final da seção 4.7, trataremos do anel de arestas  $k[G]$ , onde  $G$  é um grafo. O leitor é instado a rever os preliminares da seção 3.6.

A noção que nos norteará é a de suspensão de um grafo, a ser definida. Para habituar o leitor à linguagem algébrica, daremos a construção no contexto do ideal de Petersen.

(4.4.1) DEFINIÇÃO. Seja  $G$  um grafo com  $n$  vértices e  $k[G] = k[\underline{X}]/I(G)$ , o anel de Petersen de  $G$ . Introduzamos um novo conjunto de indeterminadas  $\underline{Y}$ , independentes de  $\underline{X}$ , tal que  $\#\underline{Y} = \#\underline{X}$ . A *suspensão* de  $G$  é o grafo cujo anel de Petersen é

$$k[\underline{X}, \underline{Y}]/(I(G) + (X_1Y_1, \dots, X_nY_n)).$$

A notação, salvo conflito, será  $S(G)$ .

A suspensão foi usada, sem esta designação explícita, por Fröberg [Frö82], Villarreal [Vil90] e Simis-Ulrich-Vasconcelos [SiUIVa90]. Em cada uma destas referências, ela veio resolver um problema diferente. Olhada de um certo ângulo, ela resolve o problema da *Cohen-Macaulização* de um grafo, através de uma construção simples mas às custas da duplicação do número de vértices.

Assim como no caso de um complexo simplicial, dizemos que um grafo  $G$  é um grafo de *Cohen-Macaulay* se o anel  $k[G]$  for de Cohen-Macaulay.

Eis, então, a principal propriedade da suspensão.

(4.4.2) PROPOSIÇÃO. *Se  $G$  é um grafo, a suspensão  $S(G)$  é um grafo de Cohen-Macaulay.*

DEMONSTRAÇÃO: ([Vil90]) (Esboço) Primeiramente, observemos que nenhuma das condições equivalentes de (4.1.2) é facilmente verificável. Mas, o candidato natural existe, a saber, a sequência diagonal

$$\underline{X} - \underline{Y} := X_1 - Y_1, \dots, X_n - Y_n.$$

De fato,  $\underline{X} - \underline{Y}$  é pelo menos um sistema de parâmetros, uma vez que a redução neste caso é

$$(4.4-1) \quad \begin{aligned} k[\underline{X}, \underline{Y}]/(I(S(G)), \underline{X} - \underline{Y}) &\simeq k[\underline{X}, \underline{Y}]/(I(G), X_1 Y_1, \dots, X_n Y_n, \underline{X} - \underline{Y}) \\ &\simeq k[\underline{X}]/(I(G), X_1^2, \dots, X_n^2) \end{aligned}$$

e o último desta cadeia de isomorfismos é de dimensão zero. Este sistema de parâmetros nos coloca, gratuitamente, na situação do lema de normalização (*Terminologia*). De fato, se  $x_1 - y_1, \dots, x_n - y_n$  denotam os resíduos de  $\underline{X} - \underline{Y}$  em  $k[S(G)]$ , então este é finitamente gerado (não só como anel, mas como *módulo*) sobre o subanel  $k[x_1 - y_1, \dots, x_n - y_n]$  pelos resíduos dos monômios

$$(4.4-2) \quad X_{i_1} \cdots X_{i_r}, \quad 1 \leq i_1 < \cdots < i_r \leq n$$

que não são divisíveis pelos geradores de  $I(G)$ .

Para completar a demonstração, usa-se um fato não trivial, que é uma (outra!) caracterização da propriedade de Cohen–Macaulay: se  $k[S(G)]$  é *livremente* gerado (quer dizer, sem dependência linear a coeficientes no subanel), então  $k[S(G)]$  é um anel de Cohen–Macaulay (vide *Terminologia*). ■

(4.4.3) EXERCÍCIO. (i) Mostre que o anel em (4.4-1) é, como se afirmou na demonstração, um anel de dimensão zero.

(ii) Experimente uma demonstração diferente de (4.4.2), tentando mostrar, por indução sobre  $n$ , que o sistema lá escolhido é uma sequência regular (mas, atenção: em  $k[S(G)]$ , não em  $k[\underline{X}, \underline{Y}]$ ).

(iii) Mostre que os geradores (4.4-2) são linearmente independentes a coeficientes no subanel  $k[x_1 - y_1, \dots, x_n - y_n]$ .

(iv) Familiarize-se com seu exemplo preferido de suspensão (o autor, por exemplo, gosta da suspensão de um ciclo impar...).

Ainda por analogia com o caso dos complexos simpliciais, diremos que um grafo é *puro* se o ideal de Petersen  $I(G)$  for puro, isto é, se todos os ideais primos mínimos deste ideal tiverem a mesma altura.

(4.4.4) COROLÁRIO. A suspensão  $S(G)$  de um grafo é um grafo puro. Além disso, os ideais primos mínimos de  $I(S(G))$  são da forma

$$(X_{i_1}, \dots, X_{i_r}, Y_{i_r+1}, \dots, Y_{i_n}),$$

onde  $(X_{i_1}, \dots, X_{i_r})$  percorre o conjunto dos ideais correspondentes às coberturas de vértices de  $G$  e os conjuntos de índices

$$\{i_1, \dots, i_r\} \text{ e } \{i_{r+1}, \dots, i_n\}$$

são complementares em  $\{1, \dots, n\}$ .

DEMONSTRAÇÃO: A primeira afirmação resulta de (4.4.3), sendo um fato geral para anéis de Cohen–Macaulay residuais de anéis de polinômios. Contudo, ela resulta da segunda afirmação, que se mostra de maneira direta e será deixada para o leitor. ■

(4.4.5) EXERCÍCIO. Mostre que o radical do ideal  $I(S(G)) + (X_1 - Y_1)$  é o ideal

$$\bigcap_{P \in \text{Min } k[S(G)]} (P, X_1 - Y_1).$$

Uma das noções mais importantes de álgebra comutativa e de geometria algébrica é a de multiplicidade. Um estudo detalhado deste conceito nos tiraria do rumo principal, já que requereria outros preliminares sobre a série de Hilbert. Será suficiente considerar este conceito na situação que mais nos interessa.

(4.4.6) DEFINIÇÃO. Seja  $A = k[\underline{X}]/I$  um anel graduado homogêneo de Cohen–Macaulay de dimensão  $d$ . A *multiplicidade* de  $A$  é dada por

$$e(A) := \lim_{z \rightarrow 1} (1 - z)^d F(A, z).$$

Esta definição parece estranhamente fora de contexto, mas é, na verdade, razoável, se lembrarmos que  $F(A, z)$  é uma função racional de  $z$ . Com efeito, se  $\theta_1, \dots, \theta_d$  é um sistema de parâmetros homogêneos de  $A$ , temos por (4.1.2)(v):

$$F(A/(\theta_1, \dots, \theta_d), z) = (1 - z)^d F(A, z).$$

Mas,  $\bar{A} := A/(\theta_1, \dots, \theta_d)$  é um anel de dimensão zero, logo, pelo lema de normalização, é um espaço vetorial de dimensão finita sobre  $k$ . Segue daí que sua série de Hilbert é um polinômio. Consequentemente

$$(4.4-3) \quad e(A) = \sum_{m \geq 0} \dim_k \bar{A}_m = \dim_k \bar{A}.$$

Parece interessante experimentar com este conceito para grafos.



(4.4.7) DEFINIÇÃO. A *multiplicidade*  $e(G)$  de um grafo  $G$  é a multiplicidade do seu anel de Petersen.

A fórmula (4.4-3) fornece uma expressão inusitada para a multiplicidade de certos grafos.

(4.4.7) PROPOSIÇÃO. Se  $G$  é a suspensão de um grafo  $G_0$ , tem-se

$$e(G) = \sum_{i=-1}^{d-1} f_i(\Delta(G_0)),$$

onde  $\Delta(G_0)$  é o complexo simplicial associado a  $G_0$  e  $d = \beta_0(G_0) = \dim \Delta(G_0) + 1$ .

DEMONSTRAÇÃO: Por (4.4.2) (ou antes, pela sua demonstração), o anel  $k[\Delta]$  admite a redução

$$k[G]/(X_1 - Y_1, \dots, X_n - Y_n) \simeq k[\underline{X}]/(I(G_0), X_1^2, \dots, X_n^2).$$

Mas, uma base vetorial desta redução é constituída pelos monômios cujos suportes são faces de  $\Delta(G_0)$  (vide (3.6.3)) e que não pertencem ao ideal  $(X_1^2, \dots, X_n^2)$ , isto é, pelos monômios livres de quadrados cujos suportes são faces de  $\Delta(G_0)$ . ■

(4.4.8) EXERCÍCIO. (i) Seja  $G$  uma suspensão. Derive uma fórmula para a multiplicidade  $e(G)$  que envolva as  $f$ -coordenadas do próprio  $G$ .

(Sugestão: Use (4.1-2))

(ii) Confirme a validade da fórmula obtida no item (i) no caso da suspensão de um ciclo  $C_3$ .

(4.4.9) PROJETO. (Sistemas de parâmetros) Seja  $G$  um grafo. A existência de um vértice livre  $X_1$  de uma aresta  $X_1X_2$  de  $G$  garante que ( $\dim G \geq 1$ ) c) um sistema de parâmetros para o anel  $k[\Delta]$  pode começar com o resíduo de  $X_1 + X_2$  (isto acontecia no caso de  $G$  ser uma suspensão). Em geral, dado um vértice  $X_1$  de  $G$ , com vértices vizinhos  $X_2, \dots, X_m$ , o resíduo de  $X_1 + X_2 + \dots + X_m$  é o primeiro elemento de um sistema de parâmetros de  $k[\Delta]$  (ou de uma sequência regular deste anel, o que é a mesma coisa já que o ideal das arestas  $I(G)$  é radical). Suponhamos  $G$  de Cohen-Macaulay. O projeto consiste em continuar a sequência regular a partir do segundo

estágio e além (quando começa a existir uma diferença entre sistemas de parâmetros e sequências regulares).

Outra propriedade de uma suspensão  $G$  que falha para outros grafos de Cohen–Macaulay é a de que “quase todos” seus subgrafos da forma  $G - v$  ainda são de Cohen–Macaulay.

Qualifiquemos “quase todos” da seguinte maneira.

(4.4.10) DEFINIÇÃO. Um grafo  $G$  é *criticamente de Cohen–Macaulay* se:

- (1)  $G$  é de Cohen–Macaulay.
- (2) O conjunto

$$CM(G) := \{v \in \mathcal{V}(G) \mid G - v \text{ é de Cohen–Macaulay}\}$$

é uma cobertura de vértices de  $G$ .

Uma noção mais fraca é a de *sub-criticamente Cohen–Macaulay*, que se obtém substituindo (2) pela condição de que  $CM(G)$  seja apenas *dominante* (isto é, de que todo vértice de  $G$  esteja conectado a algum vértice pertencente a  $CM(G)$ ).

(4.4.11) PROPOSIÇÃO. Se  $G$  é uma suspensão, então  $G$  é *criticamente de Cohen–Macaulay*.

DEMONSTRAÇÃO: Se  $G$  é suspensão do grafo  $G_0$ , então, para todo vértice  $v$  de  $G_0$ ,  $G - v = S(G_0 - v)$ . Logo,  $\mathcal{V}(G_0) \subseteq CM(G)$ , o que prova a afirmação. ■

(4.4.12) OBSERVAÇÃO. É importante não esquecer a condição (1), sem a qual muitos grafos não seriam criticamente de Cohen–Macaulay.

Uma classe especial de grafos criticamente de Cohen–Macaulay é constituída pelos grafos  $G$  tais que  $CM(G) = \mathcal{V}(G)$ . O leitor poderá se convencer de que os seguintes grafos pertencem a esta família.

- (4.4.13) EXEMPLO. (i) O grafo completo  $K_n$ .  
(ii) Um grafo  $G$  tal que  $\dim G \leq 2$  e tal que  $\Delta(G)$  seja conexo.

Baclawski [Bac81b] alçou os complexos simpliciais  $\Delta$  que gozam da propriedade correspondente – isto é, tais que  $\Delta$  é de Cohen–Macaulay e  $\Delta \setminus v := \{F \in \Delta \mid v \notin F\}$  é de Cohen–Macaulay para todo vértice  $v$  de  $\Delta$  – de *complexos duplamente de Cohen–Macaulay*.

(4.4.14) EXERCÍCIO. Mostre que as seguintes condições são equivalentes para um grafo  $G$ :

- (i)  $CM(G) = \mathcal{V}(G)$ .
- (ii)  $\Delta$  é duplamente de Cohen–Macaulay.

(4.4.15) EXEMPLO. O grafo da Figura 4.2 não é criticamente de Cohen–Macaulay: para todo vértice  $v$  do triângulo mais interno de todos  $C$ ,  $G - v$  não é de Cohen–Macaulay. Contudo,  $G$  é sub-criticamente de Cohen–Macaulay pois  $CM(G) = \mathcal{V} \setminus \mathcal{V}(C)$ .

(4.4.16) OBSERVAÇÃO. A propriedade de Cohen–Macaulay para o grafo do exemplo acima, bem como para os vários subgrafos da forma  $G - v$ , foi obtida usando o programa *Macaulay* [BaSti87]. Uma abordagem teórica seria desejável, mas alertamos para a complexidade facial dos complexos simpliciais associados.

(4.4.17) EXERCÍCIO. (i) Seja  $\Delta$  o complexo das faces de um simplexo. Mostre que o complexo das cadeias  $\Delta_c(\Delta)$  é de Cohen–Macaulay.

(Sugestão: Use (4.2.8)).

(ii) Mostre que o grafo cuja realização são as diagonais do hexágono (principais e secundárias) é de Cohen–Macaulay.

(Sugestão: Use (i); observe, alternativamente, que ele se encaixa no item (ii) de (4.4.13)).

(4.4.18) EXERCÍCIO. Seja  $C_n$  um ciclo.

(i) Se  $n$  é par, mostre que  $C_n$  não é de Cohen–Macaulay.

(Sugestão: Use a observação feita na demonstração de (4.4.4)).

(ii) Se  $n$  é ímpar, mostre que  $C_n$  é puro; se  $n \leq 5$ , mostre que  $C_n$  é de Cohen–Macaulay. O que acontece se  $n = 7$ ?

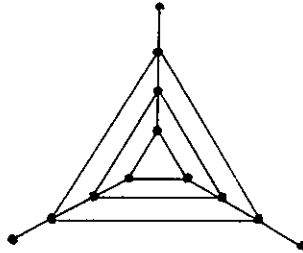


Fig. 4.2: Triângulo telescópico

**4.5 O pedestal e o tipo de um grafo.** Um somando importante da multiplicidade  $e(G)$  de uma suspensão  $G = S(G_0)$  é  $f_{d-1}(\Delta(G_0))$ , o número de facetas do complexo  $\Delta(G_0)$ . Este não é mais do que o número de conjuntos independentes máximos de  $G_0$ , mas merece ser destacado.

(4.5.1) DEFINIÇÃO. A *complexidade de independência*  $\gamma(G)$  de um grafo  $G$  é o número de conjuntos máximos independentes de  $G$ .

Equivalentemente,  $\gamma(G)$  é o número de ideais primos mínimos do ideal  $k[G]$ . Este número já foi calculado para ciclos em 2.2, mas é geralmente inacessível ao cálculo.

Daí, o interesse em caracterizá-lo algebricamente. No caso de uma suspensão, isto é possível.

(4.5.2) DEFINIÇÃO. Seja  $A = k[\underline{X}]/I$  um anel graduado de Cohen–Macaulay e seja  $\theta_1, \dots, \theta_d$  um sistema de parâmetros homogêneos de  $A$ . O *pedestal* (“socle”) de  $A$  (relativamente a  $\theta_1, \dots, \theta_d$ ) é o subespaço vetorial

$$\text{Ped}_{\theta_1, \dots, \theta_d} A := (\tilde{I} : (\underline{X})) / \tilde{I} \subset k[\underline{X}] / \tilde{I} = A / (\theta_1, \dots, \theta_d),$$

onde  $\tilde{I} + (I, \theta_1, \dots, \theta_d) \subset k[\underline{X}]$ .

Lembremos que  $(\tilde{I} : (\underline{X}))$  usa o quociente de ideais (vide *Terminologia*). A definição acima não está completa: mostra-se que dois pedestais de  $A$ , com respeito a dois sistemas de parâmetros, são isomorfos como espaços vetoriais. Isto justifica o uso da notação  $\text{Ped } A$ .

O pedestal dá origem a um número importante.

(4.5.3) DEFINIÇÃO. O *tipo* de um anel graduado de Cohen–Macaulay é a dimensão do seu pedestal.

Diremos, como em outras ocasiões, que o *tipo* de um grafo de Cohen–Macaulay é o tipo do anel de Petersen  $k[G]$ .

(4.5.4) PROPOSIÇÃO. O *tipo* de um grafo suspensão  $S(G_0)$  conexa coincide com a *complexidade de independência*  $\gamma(G_0)$ .

DEMONSTRAÇÃO: Usando o sistema de parâmetros diagonal  $\underline{X} - \underline{Y}$ , a demonstração segue o mesmo argumento empregado na prova de (4.4.7). Assim, o pedestal  $\text{Ped } k[S(G)]$  admite uma base que é um subconjunto da base de  $k[\underline{X}]/(I(G), X_1^2, \dots, X_n^2)$  constituída pelos resíduos de monômios

$$X_{i_1} \cdots X_{i_r},$$

(livres de quadrados) correspondentes a conjuntos independentes de  $G_0$ . Mas a condição de um tal monômio pertencer a  $\text{Ped } k[S(G)]$  é que, para todo  $1 \leq j \leq n$ , o monômio  $X_j \cdot X_{i_1} \cdots X_{i_r}$  seja múltiplo de  $X_j^2$  – o que é impossível, a menos que o grafo  $G_0$  seja totalmente desconexo – ou, que para todo tal  $j$ , exista  $i_t \in \{i_1, \dots, i_r\}$  tal que  $X_j X_{i_t}$  seja aresta de  $G_0$ . Mas, isto significa precisamente que o conjunto independente é máximo. ■

(4.5.5) EXERCÍCIO. Seja  $G_0$  um grafo  $r$ -partido completo, com partição  $(p_1, \dots, p_r)$ .

(i) Mostre que o tipo da suspensão  $S(G_0)$  é  $r$ .

(ii) Determine uma base vetorial explícita de  $\text{Ped } k[S(G)]$ .

A caracterização do tipo de um grafo de Cohen–Macaulay, em termos algébricos ou combinatórios, é um problema aberto. Além da suspensão, um caso que pode ser tratado é o de um grafo bipartido de Cohen–Macaulay. É de se esperar que a propriedade de Cohen–Macaulay para estes grafos constitua uma restrição considerável à sua combinatória interna.

(4.5.6) PROPOSIÇÃO. ([SiVaVi91]) *Seja  $G$  um grafo bipartido com  $n$  vértices, nenhum dos quais é isolado. Se  $G$  é de Cohen–Macaulay, existe um grafo  $G_0$  tal que:*

(i)  $\mu(I(G_0)) = \mu(I(G)) - \frac{n}{2}$ .

(ii)  $\text{Ped } k[G] \simeq \text{Ped } k[S(G_0)]$ .

*Em particular, a multiplicidade de  $G$  é*

$$e(G) = \sum_{i=-1}^{\frac{n}{2}} f_i(\Delta(G_0))$$

*e o tipo de  $G$  coincide com a complexidade de independência de  $G_0$ .*

A demonstração não é muito difícil, mas o leitor é remetido à bibliografia citada.

(4.5.7) COROLÁRIO. ([Vi90]) *Se  $G$  é uma árvore de Cohen–Macaulay, então  $G$  é uma suspensão.*

DEMONSTRAÇÃO: Mostra-se que a árvore  $G$  admite um subgrafo isomorfo ao grafo  $G_0$  obtido em (4.5.6). ■

## 4.6 Relações polinomiais.

### Relações de um ideal

Todo objeto algébrico de algum interesse admite uma *apresentação*, composta de dois ingredientes: *geradores* e *relações*. Em geral, um mesmo objeto admite apresentações diferentes, a depender da escolha dos geradores e do tipo de relação na qual se está interessado.

Nesta seção, o enfoque será nas relações do ideal de Petersen de um grafo. Contudo, a grande parte das noções aqui consideradas são extensivas a todos ideais de  $k[\underline{X}]$  (não necessariamente homogêneos numa graduação de  $k[\underline{X}]$ ). Por tal, salvo menção em contrário,  $I$  designará um ideal de  $k[\underline{X}]$ , do qual se fixou um conjunto de geradores  $\underline{f} := \{f_1, \dots, f_m\}$ .

(4.6.1) DEFINIÇÃO. (i) **Sizigias.** São as relações de  $I$ , quando este é considerado como módulo sobre  $k[\underline{X}]$ . Em outras palavras, uma *sizigia* de  $\underline{f}$  é uma  $m$ -upla (ou um  $m$ -vetor)  $(g_1, \dots, g_m)$ , onde  $g_i \in k[\underline{X}]$ , tal que

$$\sum_{i=1}^m g_i f_i = 0.$$

(ii) **Relações algébricas homogêneas.** São os polinômios

$$F(T_1, \dots, T_m) \in k[\underline{X}][\underline{T}],$$

a coeficientes em  $k[\underline{X}]$  e homogêneos em novas variáveis  $\underline{T}$ , tais que

$$F(f_1, \dots, f_m) = 0.$$

(iii) **Relações polinomiais.** São os polinômios  $P(\underline{T}) \in k[\underline{T}]$ , a coeficientes em  $k$ , nas novas variáveis  $\underline{T} = T_1, \dots, T_m$  (não necessariamente homogêneos), tais que

$$P(f_1, \dots, f_m) = 0.$$

As sizigias de  $\underline{f}$  também são chamadas *relações lineares* uma vez que correspondem, bijetivamente, às relações algébricas homogêneas  $\underline{T}$ -lineares de  $\underline{f}$ . Assim, (i) pode ser incluída em (ii) – mas, nem sempre é conveniente fazê-lo! Quanto a (iii), é de outra natureza, em geral. Evidentemente, as relações *homogêneas* em (iii) estão incluídas em (ii) – mas, podem não existir!

## Modelos triviais

Cada uma das noções em (4.6.1) admite (pelo menos) um modelo trivial, que serve como referencial para os demais casos. Novamente, a discussão é completamente geral para ideais de  $k[\underline{X}]$ . No entanto, visando simplificar as idéias, suporemos doravante que os geradores  $\underline{f}$  de  $I \subset k[\underline{X}]$  são homogêneos.

(4.6.2) DEFINIÇÃO. Os geradores  $\underline{f}$  são *sizigeticamente triviais* se toda sizigia de  $\underline{f}$  é combinação linear, a coeficientes em  $k[\underline{X}]$ , das sizigias *triviais*

$$s_{ij} := (0, \dots, 0, \underset{i}{f_j}, 0, \dots, 0, -\underset{j}{f_i}, 0, \dots, 0), \quad 1 \leq i < j \leq m.$$

Este modelo não é novo. De fato, pode-se mostrar:

(4.6.3) PROPOSIÇÃO. *As seguintes condições são equivalentes para  $\underline{f}$ :*

(i)  $\underline{f}$  é *sizigeticamente trivial*.

(ii)  $\underline{f}$  é uma  $k[\underline{X}]$ -sequência.

(4.6.4) OBSERVAÇÃO. A implicação (ii)  $\Rightarrow$  (i) é laboriosa, mas pode ser obtida por indução sobre  $m$ , a partir das definições. A implicação inversa é de outro nível de dificuldade. A não regularidade de  $\underline{f}$  traduz, no fundo, uma obstrução de caráter homológico, onde a homologia em questão é a *homologia de Koszul* (distinta de todas aquelas consideradas por ocasião do teorema (4.2.6)).

As relações algébricas homogêneas admitem mais de um modelo trivial, por ordem de enfraquecimento. Na verdade, uma boa parte dos trabalhos em álgebra comutativa ocupa-se das interações entre estes modelos, para classes específicas de ideais.

Surpreendentemente, um destes modelos triviais é já dado por uma  $k[\underline{X}]$ -sequência. Primeiro, o modelo:

(4.6.5) DEFINIÇÃO. Os geradores  $\underline{f}$  são *algebricamente triviais* se toda relação algébrica homogênea de  $\underline{f}$  pertence ao ideal

$$(f_j T_i - f_i T_j)_{1 \leq i < j \leq m} \subset k[\underline{X}, \underline{T}].$$

Agora, a surpresa:

(4.6.6) PROPOSIÇÃO. As seguintes condições são equivalentes para  $\underline{f}$ :

(i)  $\underline{f}$  é algebricamente trivial.

(ii)  $\underline{f}$  é uma  $k[\underline{X}]$ -sequência.

Desta feita, se usarmos a implicação difícil de (4.6.3), juntamente com a identificação das sizíguas com as relações algébricas  $\underline{T}$ -lineares, obteremos a implicação (i)  $\Rightarrow$  (ii) da presente proposição. A outra implicação requer uma indução tecnicamente complicada, não sendo razoável transcrevê-la aqui. Um caso particular é proposto no próximo exercício.

(4.6.7) EXERCÍCIO. Seja  $\underline{f}$  uma  $k[\underline{X}]$ -sequência constituída de dois elementos. Mostre que  $\underline{f}$  é algebricamente trivial.

Eis um outro modelo trivial mais sutil.

(4.6.8) DEFINIÇÃO. Os geradores  $\underline{f}$  de um ideal  $I \subset (\underline{X})$  são *analiticamente independentes* se toda relação algébrica homogênea pertence ao ideal do anel  $k[\underline{X}, \underline{T}]$  gerado por  $\underline{X}$ .

É imediato que trivialidade algébrica implica em independência analítica. A recíproca não é verdadeira, o que se pode ver por exemplos não muito sofisticados (exercício abaixo). À medida que nos inserimos em classes de ideais com comportamento mais especial, a validade da recíproca pode tornar-se um problema interessante.

(4.6.9) EXERCÍCIO. (i) Mostre que os polinômios  $XY, XZ \in k[X, Y, Z]$  são analiticamente independentes, mas não constituem uma  $k[X, Y, Z]$ -sequência.

(ii) Analise a questão análoga para os polinômios  $XY, XZ, YZ$ .

Finalmente, chegamos a um modelo trivial para o terceiro tipo de relação.

(4.6.10) DEFINIÇÃO. Os geradores  $\underline{f}$  são *algebricamente* (ou *polinomialmente*) *independentes* se a única relação polinomial (enfatizemos, a coeficientes em  $k$ ) é o polinômio nulo.

(4.6.11) EXERCÍCIO. Mostre que os polinômios  $X^2, XY, Y^2$  não são algebricamente independentes, mas que todas suas relações polinomiais são múltiplas de uma mesma relação fixa.



## Aneis modelos de relações

Suporemos, a partir de agora, que os geradores  $\underline{f}$  são mínimos, no sentido de que nenhum deles pertence ao ideal gerado pelos restantes (isto não representa simplificação essencial nas definições).

A fim de melhor entender as zonas de influência mútua entre as três noções de relações, é conveniente modelá-las por aneis residuais.

(4.6.12) DEFINIÇÃO. O anel (ou álgebra) que modela (ou governa) as sizigias de  $\underline{f}$  é a *álgebra simétrica*

$$\mathcal{S}(\underline{f}) := k[\underline{X}, \underline{T}] / L(\underline{f}),$$

onde  $L(\underline{f})$  é o ideal gerado pelas formas  $\underline{T}$ -lineares  $\sum g_i T_i$  correspondentes às sizigias  $(g_1, \dots, g_m)$  de  $\underline{f}$ .

(4.6.13) DEFINIÇÃO. A álgebra que governa as relações algébricas homogêneas de  $\underline{f}$  é a *álgebra de Rees*

$$\mathcal{R}(\underline{f}) := k[\underline{X}, \underline{T}] / J(\underline{f}),$$

onde  $J(\underline{f}) := ( \{ F(\underline{T}) \in k[\underline{X}][\underline{T}] \mid F(\underline{f}) = 0, F \text{ } \underline{T} \text{-homogêneo} \} )$ .

Conforme observado mais acima, tem-se  $L(\underline{f}) \subseteq J(\underline{f})$ . Por outro lado, toda relação algébrica  $\underline{T}$ -linear pertence a  $L(\underline{f})$ . Isto significa que o ideal  $L(\underline{f})$  se identifica com a parte graduada de grau 1 do ideal homogêneo  $J(\underline{f})$ .

Um ponto importante é que ambas as álgebras admitem versões intrínsecas, quer dizer, dependentes apenas de  $I$  e não dos geradores  $\underline{f}$  escolhidos. A álgebra simétrica admite uma propriedade universal característica, remanescente da de um anel de polinômios (vide *Terminologia*) e pode ser introduzida mediante um processo de *simetrização* das potências tensoriais do ideal  $I$  – tudo isto pode ser visto num primeiro curso de álgebra, mas não terá muito sentido neste.

Quanto à álgebra de Rees, a propriedade universal é mais sutil, mas, a título de compensação, ela admite uma estrutura de subanel graduado do anel  $k[\underline{X}][t]$ , este com a graduação em que  $t$  é uma variável de grau 1 e os elementos de  $k[\underline{X}]$  são de grau zero. A saber, temos

$$\mathcal{R}(\underline{f}) \simeq k[\underline{X}] + (\underline{f})t + (\underline{f})^2 t^2 + \dots \subset k[\underline{X}][t].$$

Esta identificação ainda não mostra que  $\mathcal{R}(\underline{f})$  depende só do ideal  $(\underline{f})$ . Precisamos de mais um passo, que será deixado como tarefa no exercício abaixo.

Doravante, falaremos da álgebra simétrica (respectivamente, de Rees) do ideal  $I$ , mudando as notações para  $\mathcal{S}(I), \mathcal{R}(I), L = L(I), J = J(I)$ . A inclusão  $L \subseteq J$  induz um homomorfismo sobrejetor (cf. *Terminologia*)

$$(4.6-1) \quad \mathcal{S}(I) \longrightarrow \mathcal{R}(I)$$

cujo núcleo é uma medida do fracasso das relações algébricas homogêneas em serem geradas pelas  $\underline{T}$ -lineares.

(4.6.14) DEFINIÇÃO. O ideal  $I$  será dito ser de *tipo linear* se o homomorfismo (4.6-1) for injetor.

Esta terminologia foi proposta pela escola genovesa de L. Robbiano e G. Valla.

(4.6.15) EXERCÍCIO. Mostre a plausibilidade da seguinte construção abstrata da álgebra de Rees de um ideal  $I \subset k[\underline{X}]$ .

(i) A soma direta externa das potências  $I^i$  de  $I$ , consideradas como subgrupos do grupo aditivo de  $k[\underline{X}]$ , é o grupo abeliano cujos elementos são as sequências  $(p_0, p_1, \dots)$  nulas a partir de algum  $i$  (que depende da sequência), com a soma usual coordenada a coordenada.

(ii) A soma direta em (i) admite uma estrutura de anel cuja multiplicação é induzida pelas inclusões  $I^i I^j \subset I^{i+j}$ .

(iii) O anel em (ii) é graduado, mediante uma graduação que coloca as coordenadas  $i$ -ésimas dos elementos do anel na parte graduada de grau  $i$ .

(iv) O anel graduado em (iii) é isomorfo á álgebra de Rees  $\mathcal{R}(\underline{f})$ , para qualquer conjunto  $\underline{f}$  de geradores de  $I$ .

Voltemo-nos, finalmente, às relações polinomiais de  $\underline{f}$ . Neste caso, a independência dos geradores escolhidos se coloca *a priori*, observando que temos uma subálgebra  $k[\underline{f}] \subseteq k[\underline{X}]$  e que, como se verifica facilmente, é a mesma para qualquer sistema de geradores do ideal  $I = (\underline{f})$ .

As relações polinomiais de  $\underline{f}$  geram o núcleo  $K = K(I) = K(\underline{f})$  do homomorfismo sobrejetor

$$k[\underline{T}] \longrightarrow k[I] = k[\underline{f}] \subset k[\underline{X}].$$

A álgebra que governa as relações do último tipo é, por conseguinte, a álgebra

$$\mathcal{P}(I) := k[\underline{T}]/K \simeq k[I],$$

que não tem uma designação particular, mas que bem poderia ser chamada de *segunda álgebra fundamental* devido a sua ligação com o segundo teorema fundamental da teoria dos invariantes (cf. *Palimpsestos 1, 2*).

Os três ideais  $L(I)$ ,  $J(I)$ ,  $K(I)$  serão chamados *ideais de apresentação* (da álgebra ou do tipo de relação respectivos).

A seguir, dois momentos clássicos do ideal de apresentação da segunda álgebra fundamental.

(4.6.16) EXEMPLOS. (i) (**Veronese**  $(d, r) = (d, 2)$ ) Seja  $I \subset k[\underline{X}]$  o ideal gerado por todos os monômios de grau 2 em  $\underline{X}$ . Então, a segunda álgebra fundamental de  $I$  é  $k[\underline{T}]/I_2(\mathcal{S}_2(\underline{T}))$ , onde

$$\underline{T} := \{T_{ij}\}_{1 \leq i < j \leq n}$$

e  $I_2(\mathcal{S}_2(\underline{T}))$  é o ideal gerado pelos subdeterminantes  $2 \times 2$  da matriz genérica simétrica

$$\begin{pmatrix} T_{11} & T_{12} & \dots & T_{1n} \\ & T_{22} & \dots & T_{2n} \\ & & \ddots & \vdots \\ & & & T_{nn} \end{pmatrix}.$$

(O caso  $d = 2$  é o Exercício (4.6.11)).

(ii) (**Segre**  $(r, s)$ ) Consideremos o ideal  $I \subset k[\underline{X}, \underline{Y}]$  gerado pelos monômios  $X_i Y_j$ ,  $1 \leq i \leq r$ ,  $1 \leq j \leq s$ , onde  $\#\underline{X} = r$  e  $\#\underline{Y} = s$ . Então, a segunda álgebra fundamental é  $k[\underline{T}]/I_2(\underline{T})$ , onde  $\underline{T} := \{T_{ij}\}_{1 \leq i \leq r, 1 \leq j \leq s}$  e  $I_2(\underline{T})$  é gerado pelos subdeterminantes  $2 \times 2$  da matriz (completamente) genérica retangular

$$\begin{pmatrix} T_{11} & T_{12} & \dots & T_{1s} \\ T_{21} & T_{22} & \dots & T_{2s} \\ \vdots & \vdots & \dots & \vdots \\ T_{r1} & T_{r2} & \dots & T_{rs} \end{pmatrix}.$$

(4.6.17) EXERCÍCIO. Em ambos exemplos acima mostre que o ideal gerado pelos subdeterminantes  $2 \times 2$  está contido no ideal de apresentação da álgebra fundamental respectiva.

(4.6.18) OBSERVAÇÃO. Nos exemplos (4.6.16), a álgebra fundamental faz jus a esta terminologia, no sentido de que, juntamente com as relações algébricas  $\underline{T}$ -lineares, geram o ideal de apresentação da álgebra de Rees. Este fenômeno é mais comum do que se poderia pensar, reaparecendo no contexto das ideias de Petersen (cf. mais abaixo).

(4.6.18) EXERCÍCIO. Mostre que, se  $I \subset k[\underline{X}]$  é um ideal gerado por polinômios homogêneos do mesmo grau, então

$$\mathcal{P}(I) \simeq \mathcal{R}(I)/(\underline{X})\mathcal{R}(I).$$

### As álgebras de um grafo

A partir de agora, especializaremos a discussão anterior para o caso em que  $I = I(G)$ , onde  $G$  é um grafo.

O ponto de partida é um resultado da tese de D. Taylor (Chicago, 1966), para o que introduzimos a seguinte notação.

Dada uma sequência  $\underline{g} = g_1, \dots, g_q$  de polinômios e uma sequência não decrescente  $\underline{a} = a_{i_1}, \dots, a_{i_s}$  de números inteiros, colocamos

$$\underline{g}_{\underline{a}} := \begin{cases} g_{i_1} \dots g_{i_s}, & \text{se } \{i_1, \dots, i_s\} \subseteq \{1, \dots, q\} \\ 0, & \text{no caso contrário} \end{cases}$$

Dados monômios usuais  $M, N$ , denotaremos  $[M, N]$  o seu mínimo múltiplo comum (isto é, o produto das potências de variáveis comuns de maior grau).

(4.6.19) LEMA. (D. Taylor) *Seja  $I \subset k[\underline{X}]$  um ideal gerado por monômios  $\underline{M} = \{M_1, \dots, M_m\}$  nos  $\underline{X}$ . Seja  $J \subset k[\underline{X}, \underline{T}]$  o ideal de apresentação da álgebra de Rees de  $I$ . A parte de grau  $s$  (em  $\underline{T}$ ) de  $J$  é gerada (coeficientes em  $k[\underline{X}]$ ) pelos polinômios da forma*

$$\frac{[\underline{M}_{\underline{a}}, \underline{M}_{\underline{b}}]}{\underline{M}_{\underline{b}}} \underline{T}_{\underline{b}} - \frac{[\underline{M}_{\underline{a}}, \underline{M}_{\underline{b}}]}{\underline{M}_{\underline{a}}} \underline{T}_{\underline{a}}, \quad (4.6-2)$$

onde  $\underline{a}$  e  $\underline{b}$  representam sequências não decrescentes de  $s$  inteiros.

O leitor poderá verificar que, de fato, os polinômios (4.6-2) são relações algébricas dos monômios  $\underline{M}$ . Como sempre, a outra inclusão é que traz dificuldade e não será demonstrada no curso.

Em particular, temos as relações da forma  $\underline{T}_a - \underline{T}_b$ , onde  $\underline{M}_a = \underline{M}_b$ . Elaborando o resultado de Taylor, R. Villarreal mostrou que estas relações mais simples são suficientes para gerar as partes graduadas de  $J$  de grau  $\geq 2$ . Como consequência, obteve uma descrição do ideal de apresentação da segunda álgebra fundamental de um grafo – que, a propósito, mostra que a fixação deste autor pelos ciclos pares é insuficiente...

Para tal, seja  $G$  um grafo. Um *caminho monomial* em  $G$  é um caminho fechado de comprimento par (não necessariamente um ciclo, contudo). A menos de ordem dos geradores do ideal  $I(G)$ , um caminho monomial  $C$  induz uma relação polinomial da forma

$$\underline{T}_C := T_1 T_3 \dots T_{n-1} - T_2 T_4 \dots T_n.$$

(4.6.20) PROPOSIÇÃO. *O ideal de apresentação da segunda álgebra fundamental do ideal  $I(G) = (\underline{M})$  é gerado pelos polinômios  $\underline{T}_C$  correspondentes a caminhos monomiais  $C$  em  $G$ . Se  $G$  for bipartido, o mesmo ideal é gerado simplesmente pelos polinômios correspondentes a ciclos pares.*

DEMONSTRAÇÃO: (Esboço) O ideal em questão,  $K$ , é graduado em  $\underline{T}$ . Por indução no grau  $s$ : as relações de grau  $s = 2$ , de fato, correspondem a ciclos de ordem 4 (porque?). Em seguida, pelo resultado de Villarreal acima e por (4.6.18),  $K$  é gerado pelos binômios da forma  $\underline{T}_a - \underline{T}_b$ . Consideremos o grafo  $G_1$ , cujos vértices são os vértices de  $G$  que dividem  $\underline{M}_a$  e cujas arestas correspondem aos geradores  $M_l$  de  $I(G)$  tais que  $l \in \underline{a} \cup \underline{b}$ .

Aqui há duas possibilidades, conforme valha ou não a igualdade

$$M_{i_1} \dots M_{i_m} = M_{j_1} \dots M_{j_m},$$

para algum  $m < s$ , onde  $\underline{a} = \{i_1, \dots, i_s\}$ ,  $\underline{b} = \{j_1, \dots, j_s\}$ . No primeiro caso, tem-se

$$\begin{aligned} \underline{T}_a - \underline{T}_b &= T_{i_{m+1}} \dots T_{i_s} (T_{i_1} \dots T_{i_m} - T_{j_1} \dots T_{j_m}) \\ &\quad + T_{j_1} \dots T_{j_m} (T_{i_{m+1}} \dots T_{i_s} - T_{j_{m+1}} \dots T_{j_s}) \end{aligned}$$

e podemos usar a hipótese indutiva.

O caso restante é administrado, mostrando-se que existe um caminho monomial  $C$  tal que  $\underline{T}_a - \underline{T}_b = \underline{T}_C$ . ■

Uma consequência interessante da proposição acima é uma caracterização dos grafos  $G$  cujos ideais  $I(G)$  são de tipo linear. O resultado é devido a Villarreal [Vil90].

(4.6.21) COROLÁRIO. Se  $G$  é um grafo conexo, as seguintes condições são equivalentes:

- (i)  $I(G)$  é de tipo linear.
- (ii)  $G$  tem no máximo um ciclo (necessariamente ímpar).

DEMONSTRAÇÃO: (i)  $\Rightarrow$  (ii) De maneira geral, todo ideal de tipo linear contido em  $(\underline{X})$  satisfaz a desigualdade

$$\mu(I) \leq n = \dim k[\underline{X}].$$

Este resultado foi originalmente provado em contexto mais geral [HeSi-Va83]; aplicado ao caso especial de um grafo conexo, implica em que o grafo seja uma árvore ou tenha exatamente um ciclo. Este ciclo tem de ser ímpar, senão teríamos uma relação polinomial que não resulta das  $\underline{T}$ -lineares (porque?).

(ii)  $\Rightarrow$  (i) Resulta de (4.6.20). ■

Voltando à álgebra  $k[I(G)] \subset k[\underline{X}]$ , temos o seguinte resultado, observado por Vasconcelos.

(4.6.22) PROPOSIÇÃO. Se  $G$  é um grafo conexo, tem-se

$$\dim k[I(G)] = \begin{cases} \dim k[\underline{X}], & \text{se } G \text{ não é bipartido} \\ \dim k[\underline{X}] - 1 & \text{se } G \text{ é bipartido} \end{cases}$$

DEMONSTRAÇÃO: Suponhamos  $G$  não bipartido. Afirmamos que  $G$  contém um subgrafo gerador  $H$  (vide 1.4) que admite exatamente um ciclo e este ciclo é de ordem ímpar. Isto segue da teoria das *cordas* relacionada com árvores geradoras (cf. [Har72] e a Proposição 1.4.2). Mas, então temos por (4.6.21) que  $I(H)$  é de tipo linear e tem  $\dim k[\underline{X}]$  arestas. Resulta, assim:

$$\begin{aligned} \dim k[I(G)] &\geq \dim k[I(H)] = \dim \mathcal{R}(I(H))/(\underline{X})\mathcal{R}(I(H)) \\ &= \dim \mathcal{S}(I(H))/(\underline{X})\mathcal{S}(I(H)) \\ &= \mu(I(H)) = \dim k[\underline{X}]. \end{aligned}$$

No caso bipartido, argumento similar (vide (1.4.2)) produz um subgrafo gerador contendo um único ciclo e este é de ordem par. Neste caso, é fácil ver que  $\dim k[I(G)] = \dim k[\underline{X}]$ . ■

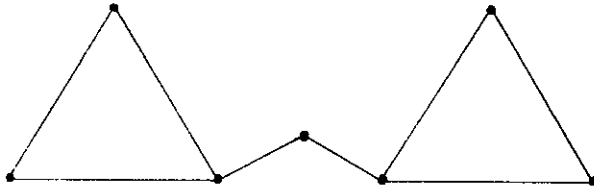


Fig. 4.3: Um caminho monomial que não é um ciclo par

(4.6.23) EXERCÍCIO. Complete a segunda parte da demonstração acima, calculando a álgebra fundamental de um ciclo par.

(4.2.24) EXEMPLO. Estude com detalhe o grafo da Figura 4.3. Pede-se exibir um caminho monomial, com a relação que lhe corresponde.

### Grafos completos

Para qualquer grafo particular, de complexidade acessível, é possível, mediante rotinas do programa *Macaulay* (cf. também *Palimpsesto 2*), calcular seus invariantes algébricos e suas álgebras de relações.

Do ponto de vista teórico, interessa-nos o comportamento típico de uma classe de grafos. Em [SiVaVi91], por exemplo, as classes de árvores, de ciclos e de grafos bipartidos foram estudadas em profundidade. No que segue, examinaremos as classes dos grafos completos e dos grafos bipartidos completos. Experimentos preliminares indicam que grafos  $r$ -partidos completos com  $n$ -vértices, onde  $3 \leq r \leq n$ , se comportam de modo diferente.

Começemos com os grafos completos.

(4.6.25) PROPOSIÇÃO. Seja  $K_n$  o grafo completo em  $n$  vértices e seja  $I_n := I(K_n)$  o anel de Petersen correspondente. Então, tem-se:

- (i)  $k[K_n] = k[\underline{X}]/I_n$  é um anel de Cohen–Macaulay de dimensão 1.
- (ii) Os primos associados de  $I_n$  são

$$(X_1, \dots, \hat{X}_i, \dots, X_n), \quad 1 \leq i \leq n.$$

(O chapéu sobre um elemento significa omissão deste elemento).

- (iii) O tipo de  $K_n$  é  $n - 1$ .

DEMONSTRAÇÃO: O resíduo da forma linear  $X_1 = \cdots + X_n$  é um elemento regular de  $k[\underline{X}]/I_n$  (porque?). A redução por este elemento fornece

$$(4.6-3) \quad \begin{aligned} k[\underline{X}]/(I_n, X_1 + \cdots + X_n) &\simeq k[\underline{X}]/((X_1, \dots, X_n)^2, X_1 + \cdots + X_n) \\ &\simeq k[\underline{X} \setminus \{X_{n-1}\}]/(X_1, \dots, X_{n-1})^2, \end{aligned}$$

que é um anel de dimensão zero (em outras palavras, um subespaço vetorial de dimensão finita). Logo,  $k[K_n]$  é de Cohen–Macaulay, de dimensão 1.

(ii) Como  $K_n$  é completo, os seus conjuntos independentes máximos são os vértices (individualmente) e os complementares destes, as coberturas de vértices mínimas. Observemos que este item implica no item (i) (porque?).

(iii) Usando a redução (4.6-3), vê-se imediatamente que

$$\begin{aligned} \text{Ped } k[K_n] &\simeq (X_1, \dots, X_{n-1})/(X_1, \dots, X_{n-1})^2 \\ &\subset k[X_1, \dots, X_{n-1}]/(X_1, \dots, X_{n-1})^2, \end{aligned}$$

de onde segue que  $\dim \text{Ped } k[K_n] = n - 1$ . ■

O teorema a seguir é o principal resultado sobre a estrutura algébrica de  $K_n$ .

(4.6.26) TEOREMA. Se  $I_n = I(K_n)$ , tem-se:

(i)  $\mathcal{R}(I_n)$  é um anel de Cohen–Macaulay.

(ii)  $k[I_n] \simeq \mathcal{R}(I_{n-1})$  (em particular, por (i), a álgebra fundamental também é de Cohen–Macaulay).

(iii) Sejam  $\underline{T} : \{T_{ij}\}_{1 \leq i < j \leq n}$  variáveis de apresentação de  $\mathcal{R}(I_n)$ . Então, o ideal de apresentação de  $I_n$  é gerado pelas relações  $\underline{T}$ -lineares e pelas relações quadráticas da forma

$$(4.6-4) \quad T_{i_1 i_2} T_{i_3 i_4} - T_{i_1 i_3} T_{i_2 i_4}, \quad T_{i_1 i_2} T_{i_3 i_4} - T_{i_1 i_4} T_{i_2 i_3},$$

duas para cada quádrupla  $\{i_1, i_2, i_3, i_4\}$  de índices distintos.

(iv) O ideal de apresentação da álgebra simétrica é radical.

DEMONSTRAÇÃO: (i) Este é um dos resultados de [SiVaVi91], onde se mostra que, de fato,  $\mathcal{R}(I_n)$  é normal (vide *Palimpsesto 2*) e usa-se um critério conhecido de Hochster [Hoc72].



(ii) e (iii) Serão demonstrados, simultaneamente, por indução sobre  $n$ , lançando mão de (i). Deixamos ao leitor a tarefa de verificar a validade de ambas as afirmações para  $n = 3$ .

Suponhamos (ii) and (iii) válidas para o caso  $n - 1$ . Ordenemos os geradores de  $I_n$  de tal maneira a ter os geradores de  $I_{n-1}$  - que é um subideal - no início. Procedemos analogamente com as variáveis de apresentação  $\underline{T}$ . Finalmente, denotemos por  $Q_n$  o ideal de  $k[\underline{X}, \underline{T}]$  gerado pelas formas (4.6-4) e lembremos que  $L(I_n) \subset k[\underline{X}, \underline{T}]$  denota o ideal gerado pelas relações  $\underline{T}$ -lineares.

Consideremos o homomorfismo sobrejetor

$$\begin{aligned} k[\underline{X}, \underline{T}] &\xrightarrow{\varphi} k[\underline{X} \setminus \{X_{n-1}\}, \underline{T} \setminus \{T_{1n}, \dots, T_{n-1n}\}] \\ T_{ij} &\mapsto T_{ij}, \quad 1 \leq i < j \leq n-1 \\ T_{in} &\mapsto X_i, \quad 1 \leq i \leq n-1 \\ \underline{X} &\mapsto 0. \end{aligned}$$

Por indução, o ideal de apresentação  $J(I_{n-1})$  da álgebra  $\mathcal{R}(I_{n-1})$  é gerado de acordo com a receita descrita em (iii). Resulta que  $\varphi(L(I_n) + Q_n) \subseteq J(I_{n-1})$ , o que induz um homomorfismo sobrejetor a nível dos anéis de resíduos

$$\begin{aligned} k[\underline{X}, \underline{T}]/(L(I_n) + Q_n, \underline{X}) &\rightarrow k[\underline{X} \setminus \{X_{n-1}\}, \underline{T} \setminus \{T_{1n}, \dots, T_{n-1n}\}]/J(I_{n-1}) \\ &\simeq \mathcal{R}(I_{n-1}). \end{aligned}$$

Este homomorfismo admite um inverso induzido pelo homomorfismo seção

$$\begin{aligned} k[\underline{X} \setminus \{X_{n-1}\}, \underline{T} \setminus \{T_{1n}, \dots, T_{n-1n}\}] &\longrightarrow k[\underline{X}, \underline{T}] \\ T_{ij} &\mapsto T_{ij}, \quad 1 \leq i < j \leq n-1 \\ X_i &\mapsto T_{in}, \quad 1 \leq i \leq n-1. \end{aligned}$$

Assim, temos

$$(4.6-5) \quad k[\underline{X}, \underline{T}]/(L(I_n) + Q_n, \underline{X}) \simeq \mathcal{R}(I_{n-1}).$$

Por outro lado, a inclusão  $L(I_n) + Q_n \subseteq J(I_n)$  induz um homomorfismo sobrejetor

$$(4.6-6) \quad k[\underline{X}, \underline{T}]/(L(I_n) + Q_n, \underline{X}) \longrightarrow k[\underline{X}, \underline{T}]/(J(I_n), \underline{X}) \simeq k[K_n]$$

onde  $\dim k[K_n] = \dim k[\underline{X}] = n$  pela Proposição 4.6.22 (a menos que  $n \leq 2$ , em cujo caso o teorema é trivial). O homomorfismo (4.6-6) resulta ser então um isomorfismo (vide *Terminologia*) e, conseqüentemente, (4.6-5) é o isomorfismo que se desejava em (ii).

Para concluir, precisamos ainda mostrar (iii). Esta parte usa a região mais fina dos conceitos de álgebra comutativa que figuram na *Terminologia*, de modo que apenas esboçaremos o argumento.

Primeiramente, afirmamos que os ideais  $L(I_n) + Q_n$  e  $J(I_n)$  têm a mesma altura e que o último é o único ideal primo *mínimo* do primeiro. Para tal, observemos o seguinte fenômeno da natureza de  $K_n$ , conseqüência de (4.6.25): para todo ideal primo  $\underline{p} \subset k[\underline{X}]$  tal que  $\underline{p} \neq (\underline{X})$ , tem-se que o localizado  $(I_n)_{\underline{p}} \subset k[\underline{X}]_{\underline{p}}$  é gerado pelas imagens de  $n - 1$  variáveis. Estas constituem, evidentemente, uma  $k[\underline{X}]_{\underline{p}}$ -sequência. Logo, pela trivialidade algébrica destas sequências ((4.6.6)), vemos que a inclusão natural

$$(L(I_n) + Q_n)_P \subseteq J(I_n)_P$$

é uma igualdade para todo ideal primo  $P \subset k[\underline{X}, \underline{T}]$  tal que  $P \cap k[\underline{X}] \neq (\underline{X})$ .

Ora, aplicando este resultado a  $P = J(I_n)$  (porque é aplicável?), obtemos

$$(L(I_n) + Q_n)_{J(I_n)} \subseteq J(I_n)_{J(I_n)}.$$

Isto mostra a afirmação feita (porque?), com uma bonificação: os outros primos da decomposição primária do ideal  $L(I_n) + Q_n$ , se existentes, contêm o ideal  $(\underline{X})k[\underline{X}, \underline{T}]$ , necessariamente. Para descartar esta possibilidade virtual, basta mostrar que alguma dentre as variáveis  $\underline{X}$  não é um divisor de zero no anel  $k[\underline{X}, \underline{T}]/(L(I_n) + Q_n)$ .

Este é o ponto nevrálgico de todo o argumento e parece uma boa ocasião para o leitor descansar.

Não existem muitos critérios para verificar se um elemento é ou não divisor de zero num anel residual de um anel de polinômios (o leitor é solicitado a dedicar alguns instantes de sua reflexão a este problema). Um dos métodos aplicáveis, principalmente no caso de elementos homogêneos de grau 1, é o das bases de Gröbner (*Palimpsesto 1*). A receita é simples: calcule-se uma base de Gröbner do ideal em questão e pince-se a lista dos monômios iniciais; o elemento é um divisor de zero relativamente ao ideal se e só se ele divide algum monômio da lista.

Acontece que só sabemos administrar bases de Gröbner para classes de ideais fortemente estruturados – por exemplo, os ideais determinantis e assemelhados. O ideal em questão,  $L(I_n) + Q_n$ , não é determinantal, mas seus geradores são, individualmente, determinantes  $2 \times 2$ . Isto ainda fornece suficiente estrutura para determinar a natureza da base de Gröbner. Precisamente:

(4.6.27) LEMA. *Os geradores de  $L(I_n) + Q_n$  acima considerados já formam uma base de Gröbner do ideal (para uma ordem conveniente das variáveis e dos monômios).*

A demonstração pode ser encontrada em [Sim91].

(iv) Mais precisamente, a afirmação é de que

$$L(I_n) = (\underline{X})k[\underline{X}, \underline{T}] \cap J(I_n).$$

Uma das inclusões é trivial. Para a outra, basta verificar que  $(\underline{X})k[\underline{X}, \underline{T}] \cap Q_n \subset L(I_n)$ . Por outro lado, tem-se  $(\underline{X})k[\underline{X}, \underline{T}] \cap Q_n = (\underline{X})Q_n$  (porque?). Então, basta demonstrar que  $Q_n \subset L(I_n) : (\underline{X})$ . Esta parte é da mesma dificuldade da obtenção da base de Gröbner e é, na verdade, uma consequência da forma explícita dos  $s$ -polinômios encontrados na trilha da base obtida. ■

O próximo teorema descreve a estrutura algébrico-analítica de um grafo bipartido completo. Este exemplo fornece um fecho adequado à seção, uma espécie de coquetel em que várias das noções do curso convergem harmoniosamente.

(4.6.28) TEOREMA. ([BrSi91], [Sim90]) *Seja  $K_{m,n}$  um grafo bipartido completo e seja  $I = I(K_{m,n}) \subset k[\underline{X}, \underline{Y}]$  ( $\#\underline{X} = m, \#\underline{Y} = n$ ) o ideal de Petersen associado. Então, tem-se:*

- (i)  $k[\underline{X}, \underline{Y}]$  admite uma estrutura de álgebra de Hodge ordinal sobre um conjunto parcialmente ordenado  $\mathcal{P}$ .
- (ii) O ideal  $I$  é gerado pelos elementos de um ideal de ordem em  $\mathcal{P}$  e este ideal é fechado por retificação.
- (iii) A álgebra de Rees e a álgebra fundamental de  $I$  são ambas de Cohen–Macaulay.

DEMONSTRAÇÃO: Primeiramente, definimos um conjunto parcialmente ordenado  $\mathcal{P}$  conveniente, a saber

$$\mathcal{P} := \{X_i, Y_j, X_i Y_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$$

munido da seguinte ordem

$$\begin{aligned} X_1 \leq \dots \leq X_m, \quad Y_1 \leq \dots \leq Y_n \\ X_{i_1} Y_{j_1} < X_{i_2} \Leftrightarrow i_1 \leq i_2, \quad X_{i_1} Y_{j_1} < Y_{j_2} \Leftrightarrow j_1 \leq j_2 \\ X_{i_1} Y_{j_1} \leq X_{i_2} Y_{j_2} \Leftrightarrow i_1 \leq i_2 \quad \text{e} \quad j_1 \leq j_2. \end{aligned}$$

Por definição, a álgebra de Hodge é *ordinal* se for governada pelo conjunto dos monômios em  $\mathcal{P}$  que não são múltiplos dos monômios da forma  $pq$ , com  $p$  e  $q$  incomparáveis. Obviamente,  $k[\underline{X}, \underline{Y}]$  é gerado pelos elementos de  $\mathcal{P}$ . Verifiquemos os axiomas  $H_1$  e  $H_2$  (vide 3.1).

Os monômios não básicos indivisíveis são da forma  $pq$ , com  $p, q \in \mathcal{P}$  incomparáveis. Na presente situação, estes são (vide Figura 4.4):

$$\begin{aligned} X_{i_1} Y_{j_1} \cdot X_{i_2}, \quad i_1 > i_2 \\ X_{i_1} Y_{j_1} \cdot Y_{j_2}, \quad j_1 > j_2 \\ X_{i_1} Y_{j_1} \cdot X_{i_2} Y_{j_2}, \quad i_1 > i_2 \quad \text{ou} \quad j_1 > j_2. \end{aligned}$$

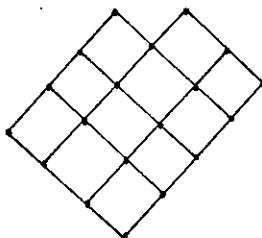


Fig. 4.4: O diagrama de Hasse de  $\mathcal{P}$

As retificações respectivas são

$$\begin{aligned} X_{i_1} Y_{j_1} \cdot X_{i_2} &= X_{i_2} Y_{j_1} \cdot X_{i_1} \\ X_{i_1} Y_{j_1} \cdot Y_{j_2} &= X_{i_1} Y_{j_2} \cdot Y_{j_1} \\ X_{i_1} Y_{j_1} \cdot X_{i_2} Y_{j_2} &= \begin{cases} X_{i_2} Y_{j_1} \cdot X_{i_1} Y_{j_2}, & \text{se } i_1 > i_2, j_1 \leq j_2 \\ X_{i_1} Y_{j_2} \cdot X_{i_2} Y_{j_1}, & \text{se } i_1 \leq i_2, j_1 > j_2 \\ X_{i_2} Y_{j_2} \cdot X_{i_1} Y_{j_1}, & \text{se } i_1 > i_2 \text{ e } j_1 > j_2 \end{cases} \end{aligned}$$

Isto mostra que  $H_1$  é preenchido e, a título de bonificação, prova que os monômios básicos geram  $k[\underline{X}, \underline{Y}]$  como  $k$ -espaço vetorial (porque?).

Quanto à independência linear dos monômios básicos, observemos que estes são, *a fortiori*, monômios usuais em  $\underline{X}, \underline{Y}$ . Como estes são linearmente independentes, basta mostrar que se dois monômios básicos

$$M_{i_1}^{d_{i_1}} \dots M_{i_r}^{d_{i_r}} \quad \text{e} \quad M_{j_1}^{e_{j_1}} \dots M_{j_s}^{e_{j_s}}$$

são iguais (como monômios usuais) então, não pode haver “embaralhamento”, isto é, deve acontecer, necessariamente,  $r = s$ ,  $M_{i_1} = M_{j_1}$ ,  $d_{i_1} = e_{j_1}$ , etc. Deixamos ao leitor a tarefa de formular este argumento cuidadosamente, deixando-se guiar, inicialmente, por exemplos construídos no diagrama de Hasse de  $\mathcal{P}$ .

(ii) Sabemos que  $I$  é gerado pelos monômios  $X_i Y_j$ . Estes constituem, como se verifica facilmente, um ideal de ordem em  $\mathcal{P}$ . Dizer que o ideal é fechado por retificação significa, por definição, que nas relações de retificação dos monômios indivisíveis  $pq$ , com  $p, q$  arestas de  $K_{m,n}$ , todo monômio básico do lado direito da relação admite dois fatores (pelo menos) que são também arestas de  $K_{m,n}$ .

Ora, esta propriedade foi estabelecida nas relações acima.

(iii) A álgebra fundamental de  $I$  já foi mencionada no Exemplo 4.6.16, (ii). Quanto à álgebra de Rees, o argumento é mais sutil e depende do fato que, para ideais fechados por retificação em álgebras de Hodge ordinais, a álgebra de Rees associada é ainda uma álgebra de Hodge – este resultado é devido a Eisenbud–Huneke, cf. [BrVe88].

O segundo ingrediente é que álgebras de Hodge sobre conjuntos parcialmente ordenados com a propriedade de ser localmente superiormente semi-modulares e auto-recobráveis, são de Cohen–Macaulay [BrVe88], (9.12). ■

(4.6.29) OBSERVAÇÃO. É possível, ainda com métodos desta natureza, concluir que os ideais de apresentação de outras álgebras que se associam têm propriedades interessantes. Por exemplo, o do cone normal de  $I$  é um ideal radical; o da álgebra de Rees *estendida* é gerada pelos subdeterminantes  $2 \times 2$  de uma matriz genérica. Mediante este último, reobtem-se todos os resultados clássicos sobre tais ideais determinantis. Para detalhes, o leitor é remetido a [BrSi91].

# APÊNDICE

## PENTIMENTO

## Apêndice. Pentimento

### PALIMPSESTO 1: TEORIA DOS INVARIANTES

**1.1 Variedades tóricas e politopos.** Uma variedade tórica é uma variedade algébrica obtida através de uma ação de um toro algébrico. Para o objetivo inicial desta seção, a definição seguinte é suficiente.

São dados dois inteiros  $n, d$  e um conjunto de pesos  $\Pi = \{w_1, \dots, w_n\} \subset \mathbb{Z}^{d-1} \times \{1\}$  tal que  $\Pi$  gera  $\mathbb{R}^d$  linearmente. Estes dados definem uma ação do grupo  $(\mathbb{C}^*)^d$  (chamado *toro algébrico*) em  $\mathbb{C}^n$ , induzida pela ação estrutural de  $GL(n, \mathbb{C})$ , através do seguinte homomorfismo “diagonal”

$$\underline{u} = (u_1, \dots, u_d) \mapsto \underline{u}^\Pi := \begin{pmatrix} \underline{u}^{w_1} & & \\ & \ddots & \\ & & \underline{u}^{w_n} \end{pmatrix},$$

onde  $\underline{u}^{w_i} = u_1^{w_{i1}} \dots u_d^{w_{id}}$ ,  $1 \leq i \leq d$ .

Como  $\Pi \subset \{X_d = 1\}$ , resulta uma ação induzida de  $(\mathbb{C}^*)^d$  no espaço projetivo  $\mathbb{P}^{n-1}$ . A *variedade tórica de peso  $\Pi$*  é o fecho da órbita do vetor  $(1, \dots, 1)$  sob esta ação.

Variedades tóricas são importantes na teoria dos invariantes e têm propriedades combinatórias notáveis. Deste ponto de vista, seu anel de coordenadas graduadas é o anel de invariantes

$$\mathbb{C}[\underline{X}]^\Pi \subset \mathbb{C}[\underline{X}]$$

da ação descrita. O célebre “Segundo Teorema Fundamental” é a descrição do ideal das relações polinomiais de  $\mathbb{C}[\underline{X}]^\Pi$ , isto é, do núcleo do homomorfismo

$$\mathbb{C}[\underline{T}] \longrightarrow \mathbb{C}[\underline{X}, 1/\underline{X}], \quad T_i \mapsto \underline{X}^{w_i}, \quad 1 \leq i \leq n.$$

Enfatizamos que o homomorfismo é a valores no anel de Laurent, não necessariamente no anel de polinômios.

Vejamos alguns exemplos para esclarecer a teoria.

(T.1) EXEMPLO. Curvas monomiais em  $\mathbf{P}^n$ .

Por simplicidade, suporemos  $n = 3$ , que já contém a dificuldade do caso geral. O toro em questão é de dimensão dois. O conjunto de pesos é da forma  $\Pi = \{(0, 1), (c, 1), (b, 1), (a, 1)\}$ , onde  $a > b > c > 0$  e  $\text{mdc}(a, b, c) = 1$ . Por exemplo, para os valores  $c = 1, b = 2, a = 3$ , obtemos a célebre cúbica reversa, cujas equações o leitor poderá suprir. Para  $c = 1, b = 3, a = 4$ , obtemos a não menos famosa quártica não normal, cujas equações, mudando os nomes das variáveis, são

$$y^3 - x^2z, \quad xw - yz, \quad z^3 - yw^2, \quad yz^2 - xw^2.$$

O estudo das curvas monomiais tem sido objeto de intensa literatura recente sobre o assunto [BrRe80], [Bre84], [CaNi83], [Eli83], [MoSi90], [MoSi91], [Sch89].

(T.2) EXEMPLO. Variedades de Veronese.

Estas são variedades “maximalistas”, num sentido que pode ser precisado. Dados inteiros  $d, r$ , os pesos são os logaritmos dos monômios de grau  $r$  em  $d$  variáveis, com a convenção de substituir a última coordenada do peso por 1. A dimensão do espaço ambiente é

$$n := \binom{d+r-1}{r} = \binom{d+r-1}{d-1}.$$

A variedade tórica correspondente é a *variedade de Veronese* (ou *veroneseana*) de tipo  $(d, r)$

O exemplo anterior pode ser obtido como projeção conveniente de veroneseanas.

(T.3) EXEMPLO. Imersões de Segre.

São dados inteiros  $r, s \geq 1$ . O conjunto de pesos é

$$\Pi_{rs} := \{(e_i, e'_j) \in \mathbb{Z}^r \times \mathbb{Z}^s \mid 1 \leq i \leq r, 1 \leq j \leq s\},$$

onde  $e_i$  (resp.  $e'_j$ ) denota o  $i$ -ésimo (resp.  $j$ -ésimo) vetor da base canônica de  $\mathbb{R}^r$  (resp.  $\mathbb{R}^s$ ).



Obtemos uma ação de  $(\mathbb{C}^*)^d$ , com  $d = r + s$ , em  $\mathbb{C}^n$ , com  $n = rs$ . A variedade tórica correspondente é chamada a *variedade de Segre* de tipo  $(r, s)$ . Observemos que o ideal da variedade é o núcleo do homomorfismo

$$\mathbb{C}[T_{ij}] \longrightarrow \mathbb{C}[\underline{X}, \underline{X}'], \quad T_{ij} \mapsto X_i X'_j.$$

Mostra-se que este ideal é gerado pelos subdeterminantes  $2 \times 2$  da matriz  $(T_{ij})$ . O exemplo mais simples corresponde aos valores  $r = s = 1$ . Neste caso, obtemos a variedade produto  $\mathbb{P}^1 \times \mathbb{P}^1$  imersa em  $\mathbb{P}^3$  de modo a coincidir com a quádriga de equação  $xw - yz$ .

O estudo destas variedades é um sub-capítulo das chamadas *variedades determinantis*, sobre as quais existe uma longa literatura clássica e moderna (vide [BrVe88] para uma familiarização com o estado d'arte da teoria).

Em seguida, tentaremos fornecer um quadro aproximado da interação entre variedades tóricas e politopos.

Existem vários politopos que se introduzem naturalmente na teoria, o mais importante sendo o politopo de pesos (ou de estado). Para melhor explicar estes objetos, convém generalizar ligeiramente a noção de variedade tórica projetiva.

Como antes, temos um toro algébrico  $T := (\mathbb{C}^*)^d$  agindo racionalmente sobre o grupo  $GL(n, V)$ , onde  $V$  é um espaço vetorial complexo de dimensão  $n$ , de tal modo que a ação contenha o subgrupo das homotetias de  $V$ . Ainda como antes, um vetor  $v \in V$  dá origem a uma variedade tórica projetiva ao se considerar o fecho da órbita  $T \cdot v$  no espaço projetivo  $\mathbb{P}(V) \simeq \mathbb{P}^{n-1}$ .

Os *pesos* da ação (ou de  $T$ ) são os vetores  $w = (w_1, \dots, w_d) \in \mathbb{Z}^d$  tais que

$$t = (t_1, \dots, t_d) \mapsto t^w = t_1^{w_1} \dots t_d^{w_d}.$$

Sabe-se, classicamente, que uma tal ação é *diagonalizável*, isto é, existe uma decomposição direta

$$V = \sum_{w \in \mathbb{Z}^d} V_w$$

onde  $V_w := \{v \in V \mid t \cdot v = t^w v, \forall t \in T\}$  é o *subespaço de peso*  $w$ .

O *suporte* do vetor  $v \in V$  é o conjunto

$$\Pi(v) := \{w \in \mathbb{Z}^d \mid V_w\text{-componente de } v \neq 0\}.$$

(T.4) DEFINIÇÃO. O *politopo dos pesos* ou o *politopo de estado* do vetor  $v \in V$  (ou ainda, da variedade  $\overline{T \cdot v}$ ) é a envoltória convexa do suporte de  $v$ . *Notação:*  $\mathfrak{P}(v)$ .

Observemos que, como antes, a hipótese sobre as homotetias garante que o suporte  $\Pi(v)$  esteja contido num hiperplano de  $\mathbb{Z}^d$ .

(T.5) EXEMPLOS. (i) **Permutaedro.** Se o vetor  $v \in V$  é genérico, no sentido de que tem coordenada não nula em  $V_w$  para todo subespaço  $V_w$  da diagonalização da ação, o politopo de estado  $\mathfrak{P}(v)$  é a envoltória convexa de todos os pesos da diagonalização. Resulta que este politopo é invariante sob a ação do grupo simétrico  $S_n$  em  $n$ . Em particular, se  $V$  é não decomponível sob a ação tórica,  $\mathfrak{P}(v)$  é simplesmente a envoltória convexa da órbita do maior peso possível, sob a ação de  $S_n$ .

Neste caso,  $\mathcal{P}(v)$  é chamado um *permutaedro*.

(ii) **Politopo de Newton.** Seja  $V = S^r(\mathbb{C}^d)$  o  $\mathbb{C}$ -espaço vetorial cuja base é constituída pelos monômios de grau  $r$  em  $d$  variáveis. Existe uma ação natural

$$GL(d, \mathbb{C}) \longrightarrow GL(n, V), \quad n = \binom{d+r-1}{r},$$

que induz uma ação tórica  $(\mathbb{C}^*)^d \longrightarrow GL(n, V)$ .

Neste caso, o politopo de estado de um polinômio homogêneo  $f \in V$  é chamado o *politopo de Newton*  $N(f)$  de  $f$ . Por definição,  $N(f)$  é a envoltória convexa dos logaritmos dos termos monomiais que ocorrem em  $f$ .

(iii) **Politopo-matroide.** Seja  $V = \wedge^r(\mathbb{C}^d)$  o espaço que parametriza o conjunto dos subespaços de dimensão  $r$  de  $\mathbb{C}^d$ . Como em (ii), temos uma ação tórica  $(\mathbb{C}^*)^d \longrightarrow GL(n, V)$ , onde  $n = \binom{d}{r}$ .

O politopo de estado de um subespaço de dimensão  $r$  de  $\mathbb{C}^d$  é chamado seu *politopo-matroide*. Os vértices do politopo admitem uma descrição em termos das célebres coordenadas de Plücker da imersão

$$\mathbb{G}(r, d) \hookrightarrow \mathbb{P}^{\binom{d}{r}-1}$$

da grassmanniana de  $r$ -subespaços.

(T.6) EXERCÍCIO. Mostre que um permutaedro pode ser identificado com a envoltória convexa do conjunto  $\{(\pi(0), \pi(1), \dots, \pi(d)) \mid \pi \in S_{d+1}\}$ .

(T.7) OBSERVAÇÃO. O estudo da grassmanniana  $\mathbb{G}(r, d)$  é o tema clássico das variedades com *air* combinatório, onde foi pioneiro o trabalho de Hodge

[HoPe52] (vide 3.2). As equações que definem  $\mathbb{G}(r, d)$  na sua imersão projetiva acima correspondem a relações de retificação da estrutura de álgebra de Hodge do anel de coordenadas homogêneas de  $\mathbb{G}(r, d)$  (vide, por exemplo, [BrVe88]).

O estudo das variedades tóricas e suas degenerações, através dos politopos de estado, é ponto alto da teoria [Oda88], [Dan78].

**1.2 Bases de Gröbner.** A noção de bases de Gröbner instalou-se, definitivamente, como um dos tópicos centrais de computação algébrica.

Gröbner, geômetra clássico, tinha uma forte sensibilidade para o lado computacional da geometria algébrica. Um dos seus alunos, Buchberger, em sua tese de Innsbruck [Buc65], abordou com sucesso um algoritmo relacionado com o cálculo de bases vetoriais de um anel de resíduos  $k[\underline{X}]/I$ .

Esta abordagem já fora considerada por Macaulay [Mac27], mas foi somente através de Buchberger – mentor incontestado das bases de Gröbner – que o tema adquiriu independência e uma carreira vertiginosa. Recolher uma bibliografia coerente na área de computação algébrica, com simpósios se sucedendo continuamente, é já em si um trabalho monumental.

Por outro lado, existem várias introduções ao assunto mais ou menos genéricas, entre outras [Buc85], [Rob90]. Uma boa parte dos trabalhos na área contém as definições aproximadas da teoria. Isto justificará, espera o autor, a não inclusão dos preliminares da teoria neste apêndice.

O objetivo desta seção é indicar, ainda que brevemente, o tratamento combinatório teórico das bases de Gröbner, tópico de recente interesse [MoRo89], [BaMo89], [StWh89], [GeKaZe89], [Stu90a], [Stu90b], [GrSt91], [KaStZe91]. Para isto, será dispensável o aspecto algorítmico da teoria. O único conceito preliminar que enunciaremos é o de ordem de termos.

(G.1) DEFINIÇÃO. Uma ordem total do conjunto de todos os termos monomiais de  $k[\underline{X}] = k[X_1, \dots, X_d]$  é dita uma *ordem de termos* se é compatível com a estrutura de semigrupo dos termos (isto é, do semigrupo aditivo  $\mathbb{N}^d$ , cujos elementos se identificam com os logaritmos dos termos).

A observação crucial sobre o significado “politópico” de uma ordem de termos foi feita por Ostrowski, num artigo de apenas duas páginas [Ost21], depois elaborada em outros trabalhos [Ost75], [MoRo89].

(G.2) PROPOSIÇÃO. Seja  $\leq$  uma ordem de termos e no anel de polinômios  $k[\underline{X}] = k[X_1, \dots, X_d]$  e seja  $D \in \mathbb{N}$ . Então existe um vetor  $(w_1, \dots, w_d) \in \mathbb{R}_{\geq 0}^d$  tal que, para todo termo de grau  $\leq D$ , tem-se:

$$\underline{X}^a < \underline{X}^b \iff \sum_{i=1}^d a_i w_i < \sum_{i=1}^d b_i w_i$$

onde  $a = (a_1, \dots, a_d)$ ,  $b = (b_1, \dots, b_d)$ .

O resultado admite também uma recíproca, que admitiremos tacitamente.

O interesse da proposição de Ostrowski é o seguinte.

Para um ideal fixo  $I$ , gerado por polinômios de grau  $\leq q$ , os polinômios numa base de Gröbner deste ideal têm seus graus limitados por  $q^{2^d}$ . Do ponto de vista computacional, uma complexidade proibitiva, que, no momento não nos diz respeito. O importante é que, como consequência da proposição, toda ordem de termos pode ser identificada com um vetor  $w \in \mathbb{R}_{\geq 0}^d$ . Um tal vetor é chamado *vetor de pesos* da ordem.

Para simplificar a discussão, suporemos que  $I$  admite geradores homogêneos (mas, advertimos que o caso não homogêneo tem suas características próprias). Lembremos, pela seção anterior, que o politopo de Newton  $N(f)$  de um polinômio homogêneo  $f$  é a envoltória convexa dos (logaritmos dos) seus termos. Por outro lado, fixada uma ordem de termos, temos a noção de *termo inicial* de  $f$ , que é o maior termo, na ordem considerada, que ocorre efetivamente em  $f$ .

(G.3) PROPOSIÇÃO. [Ost75] Os vértices de  $N(f)$  ( $f$  homogêneo) são os logaritmos dos termos iniciais de  $f$ , relativamente a todas as ordens de termos de  $k[\underline{X}]$ .

A fim de introduzir a noção análoga a de politopo de Newton para um conjunto de polinômios, utiliza-se a *soma de Minkowski* de dois politopos  $\mathfrak{P}_1, \mathfrak{P}_2 \subset \mathbb{R}^d$ :

$$\mathfrak{P}_1 + \mathfrak{P}_2 := \{v_1 + v_2 \in \mathbb{R}^d \mid v_1 \in \mathfrak{P}_1, v_2 \in \mathfrak{P}_2\}.$$

O *politopo de Newton* de um conjunto  $f = \{f_1, \dots, f_m\}$  é, então, a soma de Minkowski  $N(F) := N(f_1) + \dots + N(f_m)$ .

Diremos que duas ordens de termos são *F-equivalentes* se os termos iniciais, nas duas ordens, de cada um dos polinômios  $f_i$ ,  $1 \leq i \leq m$ , coincidem.

(G.4) PROPOSIÇÃO. [Stu91] Se  $F$  é um conjunto de polinômios homogêneos, existe uma bijeção entre os vértices do politopo de Newton  $N(F)$  e as classes de  $F$ -equivalência de ordens de termos em  $k[\underline{X}]$ .

A demonstração é técnica e é obtida passando-se aos vetores pesos das ordens. Um dos exemplos mais interessantes, tanto do ponto de vista teórico como computacional, é o chamado

(G.5) EXEMPLO. **Zonotopo.**

Se os polinômios do conjunto  $F$  são binômios, o politopo de Newton  $N(F)$  é dito ser um *zonotopo*.

Digamos,  $f_i = \underline{X}^{a_i} - \underline{X}^{b_i}$ , onde  $a_i$  e  $b_i$  designam elementos de  $\mathbb{N}^d$ . Observemos que se tem

$$N(F) = \sum_{i=1}^m \text{conv}([a_i, b_i]),$$

onde  $\text{conv}[a_i, b_i]$  denota a envoltória convexa do segmento de reta  $[a_i, b_i]$ . É possível ainda mostrar [Grü67] que existe uma outra bijeção, desta feita entre os vértices do zonotopo e as celas máximas do arranjo de hiperplanos em  $\mathbb{R}^d$  cujos vetores normais são  $a_i - b_i$ ,  $1 \leq i \leq m$ .

O último tópico que abordaremos é a relação entre as ordens de termos e os chamados *leques*, associados aos politopos através da noção de cone poliédrico. Esta última – que poderia ter sido analisada no Capítulo 2, 2.4 – pode ser encontrada, por exemplo, em [Grü67].

Dado um politopo  $\mathfrak{P} \subset \mathbb{R}^d$  e uma face  $\mathfrak{F}$  do mesmo, designamos por  $\mathcal{N}(\mathfrak{F})$  o cone poliédrico (relativamente aberto, de ápex na origem de  $\mathbb{R}^d$ ) das normais externas a  $\mathfrak{P}$  ao longo de  $\mathfrak{F}$ .

(G.6) DEFINIÇÃO. O *leque normal* de um politopo  $\mathfrak{P}$  é o complexo poliédrico (vide *Polítopos*)

$$\mathcal{N}(\mathfrak{P}) := \{\mathcal{N}(\mathfrak{F}) \mid \mathfrak{F} \text{ face de } \mathfrak{P}\}.$$

Observemos que existe uma bijeção rev-ordenada entre as faces de  $\mathfrak{P}$  e a  $(d - i)$ -celas do leque normal, dada por  $\mathfrak{P} \mapsto \mathcal{N}(\mathfrak{F})$ .

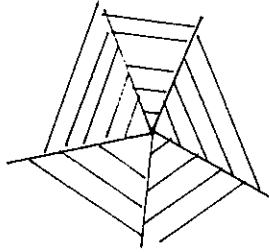


Fig Gr.1: Um leque normal

(G.7) PROPOSIÇÃO. [MoRo89] *Seja  $I \subset k[\underline{X}] = k[X_1, \dots, X_d]$  um ideal homogêneo. Então os vetores de pesos em  $\mathbb{R}^d$ , correspondentes às classes de  $I$ -equivalência de ordens de termos em  $k[\underline{X}]$ , formam um complexo poliédrico.*

O complexo poliédrico das ordens de termos é chamado *leque de Gröbner*, denotado  $\mathcal{G}(I)$ .

O fecho desta seção é o seguinte resultado, que enlaça as noções de leques normais de politopos de pesos e leques de Gröbner.

(G.8) PROPOSIÇÃO. [BaMo89] *Para todo ideal homogêneo*

$$I \subset k[X_1, \dots, X_d],$$

*existe um politopo  $\mathfrak{P}_I \subset \mathbb{R}^d$  tal que  $\mathcal{N}(\mathfrak{P}_I) = \mathcal{G}(I)$ .*

O interesse do teorema é que  $\mathfrak{P}_I$  é construído a partir do esquema de Hilbert de  $I$ , que é o objeto que parametriza os ideais homogêneos de  $k[\underline{X}]$  pelos seus respectivos polinômios de Hilbert (vide 3.7).

## PALIMPSESTO 2: POTÊNCIAS SIMBÓLICAS

**2.1 Potências simbólicas e ciclos ímpares.** As potências simbólicas de um ideal foram concebidas por W. Krull [Kru35]. Geometricamente, elas nascem da necessidade de definir, precisamente, as funções que se anulam até certa ordem ao longo de uma variedade algébrica.

A abordagem neste apêndice é inteiramente algébrica e segue a definição correntemente adotada.

(S.1.1) DEFINIÇÃO. Seja  $I \subset A := k[X]$  um ideal (homogêneo ou não) e  $m \geq 0$  um inteiro. A  $m$ -ésima potência simbólica de  $I$  é o ideal

$$I^{(m)} := I^m A_S \cap A, \quad S := A \setminus \bigcup_{P \in \text{Min } A/I} P,$$

onde  $A_S$  denota o anel de frações de  $A$  com denominadores em  $S$  (cf. *Terminologia*).

(S.1.2) OBSERVAÇÃO. (i) A definição se estende facilmente a um ideal num anel noetheriano abstrato, mas só faremos uso do caso polinomial.

(ii) A definição diz que um polinômio  $f \in A$  pertence a  $I^{(m)}$  se e só se existe  $h \in A$  tal que  $h \notin P$ , para todo  $P \in \text{Min } A/I$ , e tal que  $hf \in I^m$ .

(iii) Tem-se  $I^{(m)} \subseteq \bigcap P = \text{rad } I$ ,  $P \in \text{Min } A/I$ . Em particular, se  $I$  é um ideal radical,  $I^{(m)} \subseteq I$ . Se  $I$  é um ideal primo,  $I^{(m)}$  é exatamente a componente  $I$ -primária de  $I^m$  (cf. *Terminologia*).

(S.1.3) EXERCÍCIO. Se  $I = (f)$ , mostre que  $I^{(m)} = I^m$  pra todo  $m \geq 0$ .

(S.1.4) EXEMPLO. (Generalizando o exercício acima) Se  $I$  é um ideal homogêneo gerado por uma  $A$ -sequência, tem-se  $I^{(m)} = I^m$ , para todo  $m \geq 0$ .

O exemplo (S.1.4) é um resultado básico de álgebra comutativa, mas, de modo algum, trivial.

(S.1.5) EXERCÍCIO. (Eis como a noção funciona num caso não polinomial) Seja  $A := k[X, Y, Z]/(XY - Z^2)$  e  $I := (x, z)$ , onde  $x, z$  designam os resíduos de  $X, Z$ , respectivamente. Mostre que  $I^{(2)} = (x)$ .

Como vimos na seção 4.7, as potências ordinárias de um ideal definem a álgebra de Rees do ideal. De maneira análoga temos, para potências simbólicas.

(S.1.6) DEFINIÇÃO. A álgebra simbólica do ideal  $I \subset A$  é o anel graduado (abstrato)

$$\mathcal{R}^{(I)} := A \oplus I^{(1)} \oplus I^{(2)} \oplus \dots$$

É a primeira vez que nos deparamos com um anel graduado neste sentido, neste apêndice. Contudo, um anel semelhante foi introduzido na seção 4.6, a saber, a álgebra de Rees. Como no caso desta, a multiplicação da álgebra simbólica é induzida pela inclusão

$$I^{(r)} I^{(s)} \subset I^{(r+s)}$$

cuja verificação será deixada ao leitor.

Ainda por analogia com a álgebra de Rees  $\mathcal{R}(I)$ , a álgebra simbólica admite uma realização como sub-anel graduado do anel de polinômios  $A[t] = k[\underline{X}, t]$ :

$$\mathcal{R}^{(I)} \simeq A + I^{(1)}t + I^{(2)}t^2 + \cdots \subset A[t].$$

Doravante, salvo menção em contrário, suporemos que  $I$  é um ideal radical, em cujo caso  $I^{(1)} = I$ .

Existe uma diferença fundamental entre as duas álgebras: enquanto a álgebra de Rees é gerada pelos elementos de  $It$  (isto é, pelos seus polinômios de grau 1 em  $t$ ), o mesmo não acontece com  $\mathcal{R}^{(I)}$ . Desta forma, chegamos ao problema central da teoria das potências simbólicas.

(S.1.7) PROBLEMA. Caracterizar os ideais  $I$  para os quais  $\mathcal{R}^{(I)}$  é finitamente gerada sobre o corpo  $k$ .

Como  $\mathcal{R}(I)$  é finitamente gerada pelos polinômios  $f_1t, \dots, f_mt$ , onde  $I = (f_1, \dots, f_m)$ , e  $k[\underline{X}]$  é, evidentemente, finitamente gerado sobre  $k$ , resulta que  $\mathcal{R}^{(I)}$  é finitamente gerada sobre  $k$  se e só se ela o é sobre a sub-álgebra  $\mathcal{R}(I)$ .

Para sistematizar esta idéia, introduzimos a seguinte terminologia.

(S.1.8) DEFINIÇÃO. Seja  $I \subset k[\underline{X}]$  um ideal (radical). Um *gerador simbólico de ordem  $m$*  de  $I$  é um elemento de  $I^{(m)} \setminus I^m$ . Um gerador simbólico de ordem  $m$  é *supérfluo* se pertence ao ideal

$$II^{(m-1)} + I^{(2)}I^{(m-2)} + \cdots + I^{(\lfloor \frac{m}{2} \rfloor)}I^{(m - \lfloor \frac{m}{2} \rfloor)}.$$

Geradores não súperfluos serão ditos *genuínos*.

Nesta linguagem, dizer que  $\mathcal{R}^{(I)}$  é finitamente gerada sobre  $k$  significa que existe um inteiro  $s > 0$  tal que, para todo  $m \geq s$ , todos os geradores simbólicos de ordem  $m$  são súperfluos.

O problema da geração finita de  $\mathcal{R}^{(I)}$ , colocado nesta generalidade, é possivelmente indecidível. Para classes especiais de ideais a questão tem tido algum sucesso.

(S.1.9) TEOREMA. ([Lyu88]) *Se  $I \subset k[\underline{X}]$  é um ideal gerado por monômios livres de quadrados, então  $\mathcal{R}^{(I)}$  é finitamente gerada.*

A demonstração é engenhosa, mas não proibitivamente difícil. Remetemos o leitor ao trabalho citado.

Um dos interesses da geração finita de  $\mathcal{R}^{(I)}$  é o seguinte resultado.



(S.1.10) PROPOSIÇÃO. ([Cow85], [SiUIVa90]) Seja  $I \subset k[\underline{X}]$  um ideal homogêneo (na graduação munida de tara  $(1, \dots, 1)$ ). Seja  $\mathcal{A} \subset k[\underline{X}, t]$  um subanel graduado, finitamente gerado sobre  $k$ , tal que  $\mathcal{R}(I) \subset \mathcal{A} \subset \mathcal{R}^{(I)}$ . Então, existe um ideal homogêneo  $J \subset I$  satisfazendo as seguintes condições:

- (1)  $\mu(J) \leq \dim \mathcal{A}/(\underline{X})\mathcal{A}$ ;
- (2)  $\text{rad } J = \text{rad } I$ .

Mais uma vez a demonstração não é proibitiva, mas depende do teorema de normalização (cf. *Terminologia*). Em linguagem geométrica, a conclusão da proposição significa que a variedade algébrica definida pelos zeros do ideal  $I$  é, como conjunto, a interseção de no máximo  $\dim \mathcal{A}/(\underline{X})\mathcal{A}$  hipersuperfícies.

(S.1.11) DEFINIÇÃO. O *posto analítico* de um ideal homogêneo  $I \subset k[\underline{X}]$  é o inteiro

$$\rho(I) := \min\{s \in \mathbb{N} \mid \exists J \subset I, J \text{ homogêneo}, \mu(J) = s, \text{rad } J = \text{rad } I\}.$$

Assim, o cálculo deste invariante geométrico importante depende do comportamento íntimo das sub-álgebras de  $\mathcal{R}^{(I)}$ .

Por outro lado, todo anel graduado admite um “índice” que mede o máximo dos graus dos geradores genuínos. Um ideal admite vários destes invariantes, cada um deles correspondente a um anel graduado que se lhe associa. Em particular, temos:

(S.1.12) DEFINIÇÃO. Seja  $I \subset k[\underline{X}]$  um ideal. O *índice simbólico* de  $I$  é o menor inteiro  $s > 0$  tal que, para todo  $m \geq s$ , todo gerador simbólico de ordem  $m$  é supérfluo. Se um tal inteiro não existir, dizemos que  $I$  tem tipo simbólico infinito. *Notação*:  $s(I)$ .

O teorema de Lyubeznik (S.1.9) diz-nos que se  $I$  é gerado por monômios, vale  $s(I) < \infty$ . Reduzindo ainda mais o universo de ideais, obtem-se algum progresso além do problema central das álgebras simbólicas. Mais precisamente, perguntamos agora, no caso do ideal  $I$  ser o ideal de Petersen  $I(G)$  de um grafo  $G$ , se o índice simbólico de  $I$  pode ser expresso em termos dos invariantes combinatórios de  $G$ .

Estudo preliminar feito em [SiVaVi91] e outras evidências levam a crer que os geradores simbólicos genuínos de ordem  $m$  do ideal de Petersen de  $G$  são os monômios livres de quadrados que correspondem aos ciclos ímpares de ordem  $2m - 1$ . A título de ilustração, temos o seguinte resultado.

(S.1.13) TEOREMA. Seja  $G$  um ciclo ímpar de ordem  $n$  e  $I := I(G) \subset k[X_1, \dots, X_n]$ . Então tem-se:

- (1)  $I^{(r)} = I^r$  para  $1 \leq r \leq \frac{n+1}{2}$ .
- (2)  $X_1 \cdots X_n$  é um gerador simbólico genuíno de ordem  $\frac{n+1}{2}$  de  $I$  e é, essencialmente, único.
- (3) O índice simbólico de  $I$  é  $\frac{n+1}{2}$ .
- (4) O posto analítico de  $I$  é no máximo  $n - 1$ .

A demonstração requer alguma tecnologia que não pode ser incluída neste apêndice.

Se o grafo tem vários ciclos ímpares, possivelmente de ordens diferentes, o problema adquire complexidade. Em qualquer caso, tem-se:

(S.1.14) PROPOSIÇÃO. Se  $C$  é um ciclo ímpar de um grafo  $G$ , cujo monômio correspondente é um gerador simbólico genuíno de  $I(G)$ , então nenhuma corda de  $C$  é aresta de  $G$ .

DEMONSTRAÇÃO: Exercício. ■

Um grafo cujos ciclos ímpares sempre admitem alguma corda é um caso especial dos chamados grafos *córdicos*. Sua importância, através de (S.1.14), encontra substância no seguinte teorema.

(S.1.15) TEOREMA. As seguintes condições são equivalentes para um grafo  $G$ :

- (i) O complexo simplicial grafal associado a  $G$  é um complexo de cadeias.
- (ii) O índice simbólico de  $I(G^\perp)$  é no máximo 2, onde  $G^\perp$  denota o grafo complementar de  $G$  (vide 2.5).

A implicação (ii)  $\Rightarrow$  (i) resulta de (2.5.12). A outra implicação é mais delicada, dependendo dos métodos empregados em [SiVaVi91].

**2.2 Número cromático versus potências simbólicas.** Esta seção visa apenas complementar alguns resultados mencionados na seção anterior. Em [SiVaVi91], um resultado relativamente surpreendente foi demonstrado.

(S.1.16) TEOREMA. Seja  $G$  um grafo conexo e  $I = I(G)$  o ideal de Petersen correspondente. Então são equivalentes as duas condições:

- (i)  $G$  é bipartido.
- (ii)  $I^{(m)} = I^m$ , para todo  $m \geq 0$ .

Este resultado parece apontar na direção, senão de escrever uma fórmula exata para  $s(I(G))$  ( $G$  um grafo conexo), pelo menos de estabelecer cotas para seu crescimento.

Pelo que foi exposto na seção anterior, a noção de *cinto* (“girth”) na teoria dos grafos parece desempenhar um papel. Mais especialmente, falamos do *cinto ímpar*, como sendo a ordem do ciclo ímpar de menor ordem no grafo  $G$ . Parece não existir um consenso universal sobre a notação para designar o cinto ímpar. Usaremos o símbolo  $\sigma(G)$ .

No Capítulo 2, (2.1.12), observamos uma desigualdade básica relacionando o número cromático  $\chi(G)$  e o número de cobertura de vértices  $\alpha_0(G)$ .

Existe alguma evidência para colocar a seguinte.

(S.1.17) QUESTÃO. Se  $I$  é o ideal de Petersen de um grafo conexo  $G$ , são válidas as desigualdades

$$\max \left\{ \chi(G), \frac{\sigma(G) + 1}{2} \right\} \leq s(I) \leq \alpha_0(G)?$$

(S.1.18) EXERCÍCIO. Mostre que as desigualdades em (S.1.17) são satisfeitas no caso dos seguintes grafos:

- (i) Bipartidos (incluem árvores).
- (ii) Completos.
- (iii) Ciclos ímpares.

Relacionado com a questão acima, existe o seguinte resultado, devido a Erdős-Lovász, de cunho puramente da teoria dos grafos.

(S.1.19) TEOREMA. ([Erd61], [Lov67]) *Dados números inteiros  $r \geq 2$ ,  $s \geq 2$ , existe um grafo cujo número cromático é exatamente  $r$  e cujo cinto é pelo menos igual a  $s$ .*

Se a resposta a (S.1.17) for afirmativa, o resultado de Erdős-Lovász implicará em que o índice simbólico de um grafo seja ilimitado. Restaria mostrar, para completar o quadro, que todos os valores intermediários entre as duas cotas de (S.1.17) são de fato atingidos.

Este tipo de questão também traz à tona o problema da complexidade do índice simbólico de um grafo. Em particular, se as desigualdades em (S.1.17) – ou alguma modificação delas, envolvendo cotas parecidas – são válidas, temos o índice simbólico impressado entre dois problemas NP-completos (vide 3.3 abaixo).

**3.1 Caveat.** Dos três palimpsestos, este foi o mais impiedosamente feito durante a preparação do texto. O *caveat* refere-se, naturalmente, à intrusão de um capítulo desta natureza no texto.

Um especialista em teoria dos grafos – digamos, atuante a partir dos anos setenta – jamais se admiraria com esta inclusão, mas matemáticos mais tradicionais (o autor incluído) e, possivelmente, alunos sob sua influência, oferecem alguma resistência à heresia.

Uma justificativa simples, irrefutável mesmo, é a do gosto pessoal. O autor se inclui entre aqueles que só se sentem à vontade com uma idéia, quando a mesma se explica em padrões computacionais. Isto não significa uma renúncia à capacidade de abstração, tão característica à matemática – e, talvez, esteja aí a raiz dos mal-entendidos na questão – mas, antes, uma solidificação desta capacidade essencial.

O *caveat* vai mais além, através do fator de *evidência experimental*, que soa como uma dessas idiosincrasias emprestadas das ciências naturais, mas é apenas a utilização de métodos e algoritmos computacionais para o acúmulo de hipóteses favoráveis à formulação de teoremas virtuais.

O terceiro fator é o Século XXI.

Alguns diriam: moda. São, evidentemente, sinônimos, se usados sem ironia.

Não se concebe, perto do final deste século e início de um novo milênio, que qualquer parte da matemática e, por extensão, das ciências naturais, possa resistir ao impacto da evidência e da explicação computacional. Apesar do nível crescente de abstração da matemática, existe uma vigilante crítica (ou auto-crítica) da sua própria comunidade no sentido de, frequentemente, aferir a validade desta abstração. Isto vem acontecendo, mesmo sem a idéia subjacente da *computabilidade* do objeto matemático. Com a preocupação de um universo cada vez mais discretizado, a computabilidade será um guia inestimável.

O *caveat* chega ao seu fim. O insucesso faz parte da sua natureza. Esperamos que o leitor possa usar as duas seções seguintes para fortalecer suas impressões desta justificativa – num ou noutro sentido...

A primeira seção explica certos métodos de computação algébrica, especialmente relacionados com o sistema *Macaulay* [BaSt87]. Existe, atualmente, uma proliferação razoável de sistemas de computação algébrica. Os dois únicos sistemas dedicados completamente a tópicos de álgebra comu-

tativa, tanto quanto seja do nosso conhecimento, são *Macaulay* e *CoCoA* (este último desenvolvido na Universidade de Gênova).

A nossa preocupação não foi a de descrever o sistema ou seu funcionamento, mas de explicar como alguns dos objetos tradicionais importantes de álgebra comutativa podem ser efetivamente calculados.

A segunda seção dá uma idéia da complexidade que envolve o cálculo efetivo dos objetos, bem como da complexidade inerente a certos problemas de álgebra e de combinatória. Mais uma vez, o objetivo não foi o de discutir a complexidade, como disciplina teórica independente, mas o de se debruçar além das definições desta teoria para contemplar os “problem instances” oriundos de álgebra comutativa e combinatória.

A complexidade característica dos cálculos algébricos reside na manipulação de polinômios e das bases de Gröbner de ideais polinomiais – estas, a grosso modo, um esfacelamento completo do ideal em termos de seus polinômios. Trata-se de complexidade de tipo duplamente exponencial.

A outra, comum em combinatória, resulta de que o processo intuitivo de procura exaustiva é exponencial, ao passo que o desejável seria um processo essencialmente limitado por comportamento polinomial.

Os dois problemas não são mutuamente independentes, se bem que, no que se saiba, atualmente a sua interdependência está longe de ser entendida no detalhe.

### 3.2 Métodos e algoritmos.

#### Introdução

Computação algébrica, no sentido mais restrito do termo, distingue-se de computação simbólica geral pela sua dedicação a algoritmos que manipulam ideais polinomiais. Não existe, no momento – e, provavelmente, nunca existirá – um consenso sobre as fronteiras da computação algébrica. A título de exemplo, os algoritmos usados na teoria dos grupos finitos são, frequentemente, incluídos nesta área, embora sua preocupação central não seja a teoria dos ideais gerados por polinômios.

O pressuposto básico é um anel de polinômios  $k[X]$  sobre um corpo  $k$ . O típico algoritmo polinomial pertence à classe dos algoritmos de *forma normal*. A definição formal destes não ajudaria a compreender melhor o algoritmo e nem é a intenção do curso entrar neste mérito. No caso de polinômios, o ponto crucial é que o procedimento reconheça (fabrique, melhor dizendo), ao cabo de sua terminação, um único polinômio entre os

representantes de uma classe de equivalência. Evidentemente, a classe de equivalência que interessa é a definida por um ideal  $I \subset k[\underline{X}]$ . O método mais universalmente aceito – apesar de resultar em algoritmo de complexidade duplamente exponencial – é o da base de Gröbner, já mencionado anteriormente (*Palimpsesto 1*, 1.2).

É importante distinguir entre o dispositivo matemático de ataque ao problema e a sua implementação na máquina, através de um algoritmo. No caso, a base matemática foi lançada há cerca de 60 anos atrás, remontando a Macaulay [Mac27], Gröbner, Hermann [Her26]. O algoritmo que implementa a idéia matemática foi imaginado por Buchberger [Buc65] e seu mérito principal é o uso sistemático dos  $s$ -polinômios em conjunto com procedimentos algorítmicos de *regras de reescrever*.

A complexidade duplamente exponencial é inerente à própria teoria, não dependendo do algoritmo empregado, pelo menos no pior dos casos. Na verdade, um “pior caso” foi explicitamente construído por Mayer e Meyr [MaMe82]: trata-se de um ideal gerado por binômios nas variáveis  $\underline{X}$ , cuja complexidade de decisão para o problema da pertinência é duplamente exponencial no máximo entre o número das variáveis  $\underline{X}$  e o número de geradores do ideal.

A grande desculpa da teoria das sizíguas por tal complexidade é que o pior caso não é “matemático”, no sentido de que não pertence às grandes famílias estruturadas de ideais que gozam de razoável simetria e são centrais nas aplicações à álgebra comutativa e à geometria algébrica.

## Exemplos de objetos computáveis

Conforme mencionado mais acima, o ponto de partida de um cálculo computacional pressupõe um ambiente e um dado de entrada. Em computação algébrica *stricto-sensu*, o ambiente é um anel de polinômios  $k[\underline{X}]$ , definido através da lista de suas variáveis  $\underline{X} : X_1, \dots, X_n$  (variáveis simbólicas), ao passo que o dado de entrada é, tipicamente, um ideal  $I \subset k[\underline{X}]$ , especificado por um conjunto de geradores.

Nenhum sistema de computação algébrica vai contar muita estória sobre o ambiente polinomial: o fogo concentrado é sobre o ideal  $I$ , o qual ficará sob o assédio de rotinas diversas que calculam vários objetos associados. Entre outros, calculam-se as sizíguas de  $I$  (relações lineares dos geradores a coeficientes em  $k[\underline{X}]$ ), as equações da explosão ao longo de  $I$  (“blow-up”), as equações da fibra especial, os geradores simbólicos, os geradores

de módulos dualizantes, ideais jacobianos, explosões algébricas de Nash, grupos de cohomologia e homologia, além de invariantes e funções tais como a codimensão, a profundidade cohomológica, a dimensão homológica, a série de Hilbert, etc.

(A.1.1) EXEMPLO. A álgebra de Rees de  $I = (f_1, \dots, f_m)$ .

É o pseudônimo algébrico da explosão ao longo da subvariedade algébrica definida pelo ideal  $I$ . Por definição, esta álgebra, denotada  $\mathcal{R}(I)$ , é a álgebra de todas as relações homogêneas dos geradores  $f_1, \dots, f_m$  a coeficientes em  $k[\underline{X}]$ .

Para o seu cálculo efetivo, introduzimos novas variáveis de *apresentação*  $\underline{T} = T_1, \dots, T_m$  e uma variável  $t$  de *rotulação de grau*.

Calculada a base de Gröbner (na implementação do sistema usado) do ideal paramétrico

$$T_1 - tf_1, \dots, T_m - tf_m,$$

lá estará a sub-lista dos polinômios que não envolvem a variável  $t$ . O ideal  $J \subset k[\underline{X}, \underline{T}]$  gerado por estes define  $\mathcal{R}(I)$ .

Para calcular a fibra especial – supondo que os geradores de  $I$  são homogêneos ou têm pesos – simplesmente “matamos” todos aqueles geradores que envolvem algum coeficiente em  $k[\underline{X}] \setminus k$ . O resultado é um ideal  $K \subset k[\underline{T}]$  cujos geradores, do ponto de vista algébrico, perderam sua identidade original: não são mais relações de ninguém!

Bem, não é exatamente esta a estória. Se os geradores forem todos do mesmo grau (ou peso), então  $K$  é gerado pelas relações polinomiais de  $I$  a coeficiente em  $k$ . Não ocorrendo esta hipótese, os dois ideais,  $K$  e o ideal  $L$  gerado pelas relações polinomiais a coeficientes em  $k$ , não se aparentam muito.

(A.1.2) EXERCÍCIO. Qual a maneira de calcular o ideal  $L$ , usando o algoritmo de base de Gröbner?

Primeiramente, o cálculo de  $L$  é mais suscetível ao fatalismo da complexidade do que o de  $J$  (a definição de  $s$ -polinômio deixa claro o porque disso); em segundo lugar, mas com não menos importância, a descrição de  $L$  é objeto do célebre *Segundo Teorema Fundamental da Teoria dos Invariantes*, que consumiu bons cérebros, recuando-se até dois séculos passados.

(A.1.3) EXEMPLO. O fecho inteiro da álgebra de Rees.

É um problema mais bem inserido em aritmética. Para os geômetras, é o problema do modelo aritmeticamente normal da explosão.

O fecho inteiro tem a ver com frações racionais e estas são ainda impalatáveis no estado atual das implementações (não confundir com as rotinas de computação simbólica que manipulam frações racionais dentro de um ambiente de “algoritmo de divisão”).

Este inconveniente é contornável graças ao fato de que o ambiente  $k[\underline{X}]$  é um anel inteiro no seu corpo de frações. Substituímos o fecho inteiro de  $\mathcal{R}(I)$  pelo fecho inteiro  $\tilde{I}^r$  de cada uma das potências  $I^r$  do ideal  $I$ , assim definido:  $f \in \tilde{I}^r$  se e só se  $f \in k[\underline{X}]$  e satisfaz uma equação de dependência inteira da forma

$$f^q + g_1 f^{q-1} + \cdots + g_q = 0,$$

com  $g_i \in I^{ri}$ ,  $1 \leq i \leq q$ .

O problema não melhora, sensivelmente, com esta modificação. Na verdade, não possuímos um método matemático que permita implementar uma rotina sistemática para o cálculo destas *potências normalizadas*.

Existe um caso especial em que a rotina é possível: quando os geradores de  $I$  são monômios. Neste caso, as potências usuais ainda são geradas por monômios, obviamente, e pode-se mostrar que o fecho inteiro é essencialmente dado pelo pela *envoltória convexa* dos expoentes dos monômios geradores.

Esta envoltória convexa é, essencialmente, o politopo de Newton do ideal. A transferência deste caso para o geral, através do politopo de Newton de um ideal homogêneo, é feita através da teoria das variedades tóricas e dos seus politopos e leques de estado (vide *Palimpsesto 1*), juntamente com a teoria combinatória do esquema de Hilbert – ambos tópicos de grande efervescência moderna [Bay82], [BaMo89], [KaStZe91], [GeKaZe89], [Stu90a], [Oda88], [Dan78].

(A.1.4) EXEMPLO. Potências simbólicas de  $I$ .

Para a definição e seu contexto, vide *Palimpsesto 2*. Visando simplificar a discussão, suporemos que  $I$  é um ideal primo ou, pelo menos, radical (cf. *Terminologia*).



A situação computacional é mais favorável do que em (A.2). Na verdade, existem inclusões canônicas

$$\tilde{I}^r \subseteq I^{(r)}, \quad r \geq 0,$$

de modo que  $I^{(r)}$  é um objeto mais leniente.

Pela definição, queremos detectar polinômios  $f \in k[\underline{X}]$  satisfazendo  $gf \in I^r$ , para algum  $g \in k[\underline{X}] \setminus I$  (se  $I$  for primo). Felizmente, um dos objetos extremamente computáveis é o quociente de ideais (cf. *Terminologia*)

$$I_1 : I_2 = \{f \in k[\underline{X}] \mid fI_2 \subset I_1\},$$

que é, em sua essência, um cálculo de sizigias.

Ora, escolhido um  $g \notin I$  (em posição genérica ou aleatória), basta calcular o quociente  $I^r : (g)$ . Repetimos esta operação para vários  $g \notin I$  até estabilizar o cálculo, determinando todos os geradores de  $I^{(r)}$ .

Não se trata de uma rotina sistemática, muito menos infalível. Existe a questão de saber quando se esgotaram todos os geradores de  $I^{(r)}$  (o autor agradecerá a solução do leitor, mantendo sigilo em torno da confidência).

Novamente, podemos apontar um caso especial, em que uma rotina mecânica é possível. Suponhamos que o ideal em questão é o ideal  $I \subset k[\underline{T}]$  das relações polinomiais de um outro ideal  $(f_1, \dots, f_m)$  – um ideal de segunda geração, concordaríamos. Em princípio, então, os geradores de  $I$  foram obtidos a partir dos polinômios paramétricos  $T_1 - f_1, \dots, T_m - f_m$ . Mais precisamente,

$$I = k[\underline{T}] \cap (T_1 - f_1, \dots, T_m - f_m)$$

(a menos de considerações sobre a ordem dos termos, que não nos interessa no momento). Suponhamos que  $f_1, \dots, f_m$  sejam homogêneos (ou tenham pesos). Para muitos efeitos, os polinômios paramétricos se comportam como variáveis. Por exemplo, eles formam uma sequência regular (*Terminologia*). Para tais sequências, as potências simbólicas do ideal gerado pelos constituintes coincidem com as potências usuais – este fato não é trivial, mas é básico.

O golpe de misericórdia é observar que vale

$$I^{(r)} = k[\underline{T}] \cap (T_1 - f_1, \dots, T_m - f_m)^{(r)}, \quad r \geq 0.$$

O saldo é que, para calcular a potência simbólica  $I^{(r)}$ , basta calcular a contração em  $k[\underline{T}]$  da potência  $r$ -ésima dos polinômios paramétricos.

Trata-se de uma rotina excepcionalmente sistemática, uma vez que a contração (=interseção com um subanel de polinômios) é, uma vez escolhida a ordem adequada dos termos, um problema direto de cálculo de bases de Gröbner.

Evidentemente, paga-se o preço na complexidade, o que é inerente à teoria das sizíguas.

(A.1.5) EXEMPLO. A segunda potência simbólica.

Para  $I^{(2)}$  existe um método especial. Trata-se de um método, não de uma rotina. A consequência é de baixa complexidade computacional.

O método é baseado na teoria das diferenciais de Kähler, que são definidas (apresentadas, seria o termo exato) pela matriz jacobiana  $\partial \underline{f} / \partial \underline{X}$  dos geradores  $\underline{f}$  de  $I$ , desde que os elementos da matriz sejam “lidos módulo  $I$ ”. Parece meio estranho para o novíço, mas tem uma explicação de fundo geométrico bastante razoável.

Continuando, a teoria diz que as sizíguas de  $\partial \underline{f} / \partial \underline{X} \pmod{I}$ , consideradas como vetores-coluna de uma nova matriz  $\Phi$ , se aplicam sobre os geradores  $\underline{f} \pmod{I^2}$ . Manipulando esta situação, com técnicas algébricas básicas, não é difícil mostrar que o produto matricial  $\underline{f}\Phi$  fornece os geradores da potência simbólica  $I^{(2)}$ .

O método clama por uma extensão ao caso de potências superiores. No momento, tanto quanto seja do nosso conhecimento, não existe uma teoria para fundamentar uma rotina sistemática como a que acabamos de descrever.

**3.3 O problema da complexidade.** Começaremos por estabelecer algumas idéias sobre complexidade, fatalmente informais.

**Modelos de computação e complexidade.**

A noção de *complexidade temporal* (ingles: “time complexity”) poderia ser enunciada, informalmente, em termos de funções cujo argumento é uma *palavra de bits* (“string”) que reflete o tamanho do problema que se quer resolver computacionalmente. É evidente que isto não define nada e só pode ser usado num círculo fechado de iniciados. A definição rigorosa da terminologia de complexidade pressupõe um tratamento adequado das noções

de máquinas determinísticas e não determinísticas, que foge ao formato do curso.

Para cada um destes modelos, é possível formular as seguintes noções (esotéricas para o noviço):

(i) Programa  $M$ , com a seguinte especificação:

- (1) Um alfabeto  $\Sigma$  de *símbolos de inserção* (“input symbols”) e o conjunto  $\Sigma^*$  das palavras correspondentes;
- (2) Um conjunto  $Q$  de *estados*, incluindo dois estados de *parada*;
- (3) Uma função de transição  $\tau : Q \times \Sigma \longrightarrow Q \times \Sigma$ .

(ii) Linguagem  $L_M$  reconhecida por cada programa  $M$ ;

(iii) Problema de decisão  $\Pi$ ;

(iv) Esquema de codificação  $\Gamma$ .

Um programa  $M$  resolve o problema de decisão  $\Pi$ , sob a codificação  $\Gamma$  se  $L_M = L[\Pi, \Gamma]$ , onde  $L[\Pi, \Gamma]$  denota o conjunto das palavras usadas para codificar um exemplo do problema  $\Pi$ . Informalmente, sabemos o que significa ter computado um problema. Se  $M$  é um programa que computa um problema (isto pode ser definido, mais precisamente, em termos de estados de parada), então o *tempo* usado na computação é o número de passos até uma parada. Finalmente, a (*função de*) *complexidade temporal* de um programa  $M$  é a função  $T_M : \mathbb{N} \longrightarrow \mathbb{N}$  assim definida:

$$T_M(n) = \max\{m \mid \exists x, |x| = n, M \text{ computa } x \text{ em tempo } m\}.$$

Agora, é possível precisar o que se entende por um programa  $M$  resolúvel em *tempo funcional*  $f : \mathbb{N} \longrightarrow \mathbb{N}$ : trata-se de um programa para o qual  $T_M(n) \leq f(n)$  para todo  $n \in \mathbb{N}$ . Assim, se  $f$  for uma função linear (respectivamente logarítmica, polinomial, exponencial, duplamente exponencial, etc.), a complexidade do programa  $M$  será *linear* (respectivamente *logarítmica, polinomial, exponencial, duplamente exponencial, etc.*).

As mesmas definições funcionam no caso de um modelo não determinístico, com exceção da definição do modelo em si, que requer um módulo adicional de *tentativa* (“guessing”). Existe uma definição rigorosa disso, mas a diferença essencial para o modelo determinístico é que o programa pode (e deve) dar paradas intermediárias para *adivinhar* através do módulo de tentativa.

Do ponto de vista de complexidade funcional, não existe grande diferença entre dois modelos de computação (sempre que forem ambos determinísticos ou não determinísticos). Desta maneira, renunciamos ao detalhe do modelo, do programa e até mesmo do problema, passando a falar diretamente da complexidade de *exemplo* do problema.

Por exemplo, falaremos da complexidade de problemas (de decisão) e de classes de complexidade (algorítmica). A principal classe de complexidade é a polinomial, por razões teóricas e práticas. Por razões de clareza e tradição, estas classes recebem notações diferentes, conforme pertençam ao modelo determinístico (**P**) ou não determinístico (**NP**). Mas, a maior razão para a nomenclatura distinta é que, como classes de problemas, temos a inclusão  $\mathbf{P} \subseteq \mathbf{NP}$ . Com efeito, se  $\Pi \in \mathbf{P}$  e  $A$  é um algoritmo determinístico polinomial que decide  $\Pi$ , obtemos um algoritmo polinomial não determinístico usando  $A$  como estágio de verificação, desprezando qualquer tentativa.

### Problemas NP-completos.

A crença geral dos especialistas em complexidade é que a inclusão acima mencionada é própria. Até o momento, não se sabe se isto é verdade.

É preciso entender que, para verificar se  $\Pi \in \mathbf{NP} \setminus \mathbf{P}$  é preciso provar que algum exemplo de  $\Pi$  não admite computação em tempo polinomial em qualquer algoritmo implementado em qualquer modelo determinístico. Apesar da questão não depender deste último, a decisão é desconfortável.

Enquanto não for encontrado um tal exemplo, faz sentido procurar entender as relações entre os problemas **NP** sobre os quais *ainda* não se sabe se pertencem à classe **P**. Um dos fenômenos estranhos da teoria é que é possível afirmar várias coisas sobre estes problemas. A característica comum entre eles é que ou todos pertencem a **P** ou nenhum deles pertence a **P**!

Esta é exatamente a definição de um problema **NP** ser **NP-completo**. Por meio de uma transformação polinomial – que pode ser informalmente definida como uma transformação entre os conjuntos de exemplos de dois problemas, computável em tempo polinomial, que transforma exemplos afirmativos em exemplos do mesmo tipo – todo problema **NP-completo** é equivalente a qualquer outro problema **NP-completo**.

De modo que, o ponto alto da teoria é exhibir alguns exemplos destes problemas. Paradoxalmente, existem muitos destes exemplos, já que produzir transformações polinomiais não é muito difícil, desde que se tenha um conhecimento aprofundado do problema.

## Exemplos de problema NP-completos.

O passo inicial na teoria foi dado por S. Cook [Coo71], mostrando que o problema da *satisfatibilidade* (SAT) é NP-completo. Trata-se de um problema de álgebra booleana. É dado um conjunto  $U = \{u_1, \dots, u_n\}$  de variáveis booleanas, com as variáveis complementares,  $\bar{u}_i$  - em conjunto, chamadas *literais* - e uma função *verdade* de  $U$  num conjunto de dois elementos. Por definição, se  $u_i \in U$  é verdadeira (resp. falsa), então  $\bar{u}_i$  é falsa (resp. verdadeira). Uma *cláusula* sobre  $U$  é um conjunto finito de literais sobre  $U$ . A cláusula é dita ser *verdadeira* se ao menos um de seus literais é verdadeiro. Finalmente, uma coleção finita de cláusulas sobre  $U$  é *satisfeita* se existe uma função verdade para a qual todas as cláusulas da coleção são verdadeiras.

A demonstração de que o problema SAT é NP-completo é extremamente difícil, ao menos para este autor. Contentar-nos-emos em dar exemplos pertinentes ao curso, explicando, por meio de exemplo, uma transformação polinomial de SAT em um destes exemplos.

(C.1) PROBLEMA. Dado um grafo  $G$  e um inteiro  $k \leq n = \#\mathcal{V}(G)$ , existe uma cobertura de vértices de  $G$  cujo cardinal seja  $\leq k$  ?

Trata-se de um problema em NP, uma vez que um algoritmo não determinístico *tenta* um conjunto de vértices e testa, em tempo polinomial, se de fato o conjunto cobre todas as arestas e tem cardinal  $\leq k$ .

Para mostrar que SAT é polinomialmente transformável em (C.1), é mais fácil transformar uma variação de SAT, chamado 3SAT, em que o cardinal das cláusulas é constantemente igual a 3 - o ponto, claro, é que SAT e 3SAT são, por sua vez, polinomialmente equivalentes.

O método que apresentaremos, sem rigor ou detalhes, foi imaginado por Karp [Kar72]. Para efetuar a transformação, considera-se um caso ("instance") de 3SAT, definido por um conjunto  $U = \{u_1, \dots, u_n\}$  de variáveis booleanas (e suas negações  $\{\bar{u}_1, \dots, \bar{u}_n\}$ ) e um conjunto de cláusulas  $C = \{c_1, \dots, c_m\}$ , cada uma consistindo de 3 literais.

Com estes dados, Karp constroi um grafo  $G$ , usando a seguinte receita. Numa etapa preliminar, introduz-se um par de vértices  $\{v_i, \bar{v}_i\}$ , para cada par  $\{u_i, \bar{u}_i\}$ , e uma aresta conectando estes vértices. Similarmente, para cada cláusula  $c_j = \{u_{1j}, u_{2j}, u_{3j}\}$ , introduzimos um ciclo de ordem 3, com vértices  $\{v_{1j}, v_{2j}, v_{3j}\}$ .

O resultado, até aqui, é um grafo desconexo. Por exemplo, se o modelo do caso booleano tem 4 variáveis e duas cláusulas, então o grafo ora definido tem o aspecto da Figura Ap.1.

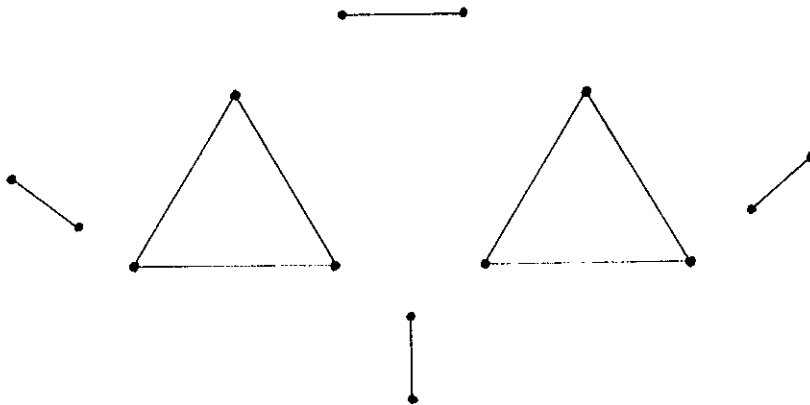


Fig. Ap.1: Grafo associado a um modelo booleano

Com esta construção provisória, transformamos o *modelo* do caso booleano, mas não o caso propriamente dito. Em outras palavras, não transformamos a informação interna de cada cláusula. Transformando apenas o modelo, obtemos apenas 1-fatores e 2-fatores do grafo definitivo.

A última etapa consiste, então, em conectar cláusulas e pares de literais, seguindo a seguinte receita natural: dada uma cláusula  $c_j$  e um literal  $u_{lj} \in c_j$ , existe um único par  $\{u_{i(l)}, \bar{u}_{i(l)}\}$  tal que  $u_{lj}$  coincide com um (e um só) dos literais deste par; introduzimos, então, uma aresta conectando o vértice  $v_{lj}$ , correspondente a  $u_{lj}$ , ao vértice correspondente ao literal do par  $\{u_{i(l)}, \bar{u}_{i(l)}\}$  que coincide com  $u_{lj}$ .

Desta forma, se o caso booleano tem 4 variáveis e, por exemplo, as duas cláusulas  $c_1 = \{u_1, \bar{u}_3, \bar{u}_4\}$ ,  $c_2 = \{\bar{u}_1, u_2, \bar{u}_4\}$ , então o grafo de Karp tem o aspecto da Figura Ap.2.

Para completar a construção, devemos definir ainda o inteiro  $k$  de teste. Fazemos  $k = n + 2m$  (porque?).

(C.2) EXERCÍCIO. O grafo de Karp pode ser desconexo? (contra-exemplo ou demonstração).

(C.3) EXERCÍCIO. Verifique a possibilidade de um caso booleano cujo grafo de Karp não admita vértices livres.

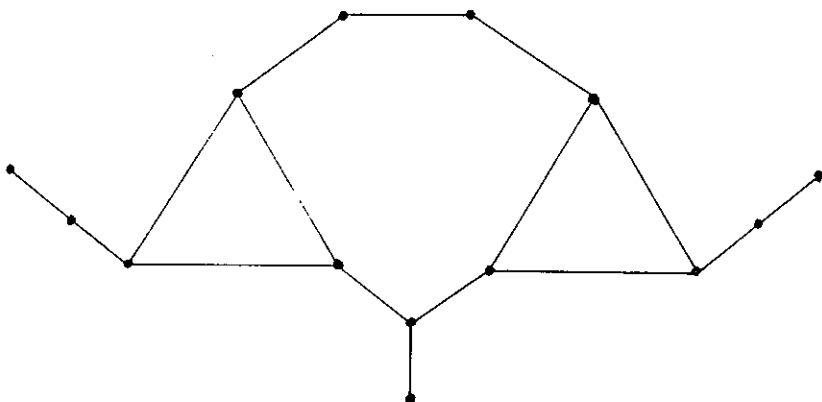


Fig. Ap.2: Grafo associado a um caso booleano

(C.4) EXERCÍCIO. Torne plausível o resultado de Karp, a saber, que o conjunto  $C$  de cláusulas do caso booleano é satisfeito se e só se o grafo de Karp admite coberturas de vértices com cardinal  $\leq n + 2m$ .

(C.5) EXERCÍCIO. Convença-se de que a transformação de Karp é, de fato, polinomial (isto é, terminável em tempo polinomial).

A seguir, um outro exemplo oriundo da teoria dos grafos.

(C.6) PROBLEMA. Dado um grafo  $G$  e um inteiro  $k \leq \#\mathcal{V}(G)$ , existe um conjunto independente de vértices de cardinal  $\geq k$ ?

Este problema, evidentemente, tem mesma complexidade de (C.1). A interseção dos dois (leia-se: a busca de coberturas independentes) pertence a  $\mathbf{P}$ . De maneira semelhante, o problema (C.2), se restringido a grafos bipartidos, pertence a  $\mathbf{P}$  [Har72].

Problema ligados à cromatização também são complexos.

(C.7) PROBLEMA. Dado um grafo  $G$  e um inteiro  $k \leq \#\mathcal{V}(G)$ , existe uma coloração com  $k$  cores?

Ainda Karp provou que  $\mathbf{3SAT}$  é polinomialmente transformável no problema (C.6).

O que intriga é que (C.3) continua  $\mathbf{NP}$ -completo para grafos planares, com  $k = 3$ , apesar da solução do problema das 4 cores [ApHa77].

Observemos que, para  $k = 2$ , o problema pertence a **P**. Também pertence a **P** a restrição do problema a grafos *córdicos*, isto é, grafos para os quais todo ciclo de ordem  $\geq 4$  admite uma corda [Gav72]. Chamamos a atenção destes dois casos pois estão intimamente relacionados com o tipo simbólico do ideal de arestas (para detalhes, vide *Palimpsesto 2*).

Nosso último problema relaciona-se com subgrafos induzidos.

(C.8) PROBLEMA. Dado um grafo  $G$  e um inteiro  $k \leq \#\mathcal{V}(G)$ , existe uma partição  $\mathcal{V}(G) = V_1 \sqcup \dots \sqcup V_k$  tal que os subgrafos induzidos pelos conjuntos  $V_i$  sejam acíclicos (isto é, florestas)?

O problema é transformável a partir de (C.7) [GaJo79]. Praticamente qualquer variação de (C.8), substituindo “floresta” por outra classe de grafos – completos, bipartidos completos, hamiltonianos, 1-fatores – é NP-completo.

Em particular, poderíamos indagar sobre a complexidade de (C.4) para subgrafos induzidos que admitam (no máximo) um ciclo ímpar em cada componente conexa. A questão tem uma contra-partida matemática interessante: dado um grafo  $G$ , qual a configuração dos subgrafos induzidos de  $G$  cujas ideias de arestas são de tipo linear? (Um ideal  $I \subset k[X]$  é dito ser de *tipo linear* se as suas relações polinomiais, a coeficientes em  $k[X]$ , são geradas pelas lineares – vide 3.2 deste *Palimpsesto* para a noção de relações polinomiais e sua complexidade).



TERMINOLOGIA DE

ÁLGEBRA COMUTATIVA

# Terminologia de Álgebra Comutativa

## ANEIS E IDEAIS, I

Todos os aneis serão comutativos, munidos de identidade multiplicativa denotada 1. Na verdade, todos os aneis considerados no curso são aneis “concretos”, isto é, aneis residuais de aneis de polinômios sobre um corpo fixo  $k$ .

### I.1 Homomorfismos de aneis.

(I.1.1) DEFINIÇÃO. Um *homomorfismo de aneis*  $\varphi : A \longrightarrow B$  é uma aplicação do anel  $A$  no anel  $B$  que preserva as duas operações estruturais e a identidade multiplicativa.

Um homomorfismo bijetor é chamado *isomorfismo*. Se  $\varphi : A \longrightarrow B$  é um isomorfismo, então a inversa de  $\varphi$  é, automaticamente, um homomorfismo. Um isomorfismo preserva tôdas as propriedades estruturais do anel de origem (mas, pode não preservar certas construções especiais).

Um subconjunto  $C \subset A$  é um *subanel* se a inclusão dos conjuntos for um homomorfismo. Um homomorfismo injetor de aneis  $A \hookrightarrow B$  permite identificar  $A$  com um subanel de  $B$ .

(I.1.2) EXEMPLO. Qualquer anel de polinômios a uma variável sobre um corpo pode ser identificado (mediante muitos homomorfismos) com um subanel de outro anel de polinômios a uma ou mais variáveis, sobre o mesmo corpo (vide I.3 abaixo).

### I.2 Ideais e aneis de resíduos.

(I.2.1) DEFINIÇÃO. Um *ideal* do anel  $A$  é um subconjunto  $I$  de  $A$ , contendo  $0 \in A$ , fechado sob a operação aditiva de  $A$  e fechado sob multiplicação por elementos de  $A$ .

Um ideal  $I \subset A$  é, geralmente, dado por um *sistema* ou *conjunto de geradores*: um subconjunto  $E \subset I$  tal que todo elemento de  $I$  se escreve na forma  $\sum a_i e_i$  (soma finita), com  $a_i \in A$  e  $e_i \in E$ . Todos os ideais considerados no curso serão *finitamente gerados*, no sentido de que existe um conjunto  $E$  finito com a propriedade acima. Neste caso, se  $E = \{e_1, \dots, e_m\}$ , usaremos

a notação  $I = (e_1, \dots, e_m)$  para indicar que o ideal  $I$  é gerado por estes elementos.

Um ideal  $I \subset A$  determina uma relação de equivalência em  $A$  definida por

$$a \equiv b \Leftrightarrow a - b \in I.$$

O conjunto das classes desta relação, denotado  $A/I$ , admite uma estrutura de anel. A saber, se  $\bar{a} \in A/I$  designa a classe do elemento  $a \in A$ , definimos  $\bar{a} + \bar{b} := \overline{a + b}$  e  $\bar{a}\bar{b} := \overline{ab}$ .

Este anel é chamado *anel de resíduos* (ou *anel das classes residuais*) de  $A$  relativamente a (ou módulo o) ideal  $I$ . Alguns livros usam a terminologia *anel quociente*, o que será evitada no curso para evitar possível confusão com os anéis de frações, às vezes chamadas quocientes, e com o quociente de dois ideais (vide abaixo).

O anel de resíduos tem uma propriedade característica, a saber:

(I.2.2) FATO. *Seja  $A$  um anel,  $I \subset A$  um ideal e  $\varphi : A \rightarrow B$  um homomorfismo. Então, existe um homomorfismo  $\bar{\varphi} : A/I \rightarrow B$  tal que  $\bar{\varphi}(a) = \varphi(a)$ , para todo  $a \in A$  se e só se  $\varphi(I) = 0$ .*

O homomorfismo  $\bar{\varphi}$  acima é dito *induzido* por (ou *residual* de)  $\varphi$ . A aplicação canônica  $A \rightarrow A/I$ , que manda um elemento na sua classe, é um homomorfismo sobrejetor. Usando este homomorfismo, é possível traduzir o Fato I.2.2 em termos de uma propriedade universal, mas não faremos uso desta faceta.

(I.2.3) EXEMPLO.  $A = \mathbb{R}[X]$ ,  $I = (X^2 + 1) \subset A$ . Então, o homomorfismo  $\varphi : A \rightarrow \mathbb{C}$  tal que  $\varphi(\alpha) = \alpha \quad \forall \alpha \in \mathbb{R}$  e tal que  $\varphi(X) = \sqrt{-1}$ , induz um homomorfismo residual  $A/I \rightarrow \mathbb{C}$  que é um isomorfismo e permite, portanto, identificar os dois anéis.

### I.3 Álgebras afins.

(I.3.1) FATO. *Seja  $k$  um corpo. O anel de polinômios a  $n$  variáveis (ou indeterminadas) sobre  $k$ , denotado  $k[\underline{X}] := k[X_1, \dots, X_n]$ , é caracterizado pela seguinte propriedade universal: dado um anel  $A$ , elementos  $a_1, \dots, a_n \in A$  e um homomorfismo (automaticamente injetor)  $\iota : k \rightarrow A$ , então existe*

um e um só homomorfismo

$$\begin{aligned}\varphi : k[\underline{X}] &\longrightarrow A \\ \varphi|_k &= \iota \\ \varphi(X_i) &= a_i, \quad 1 \leq i \leq n.\end{aligned}$$

(I.3.2) DEFINIÇÃO. Uma *álgebra* ou *anel afim* (sobre  $k$ ) é um anel residual da forma  $k[\underline{X}]/I$ , onde  $I \subset k[\underline{X}]$  é um ideal.

(I.3.3) OBSERVAÇÃO. Mais geralmente, dados anéis  $B$  e  $A$  e um homomorfismo injetor  $\iota : B \longrightarrow A$ , dizemos que  $A$  é uma  $B$ -*álgebra*. Se existir um conjunto de elementos  $a_1, \dots, a_n \in A$  tais que todo elemento  $a \in A$  se escreva na forma

$$a = \sum b_{d_1 \dots d_n} a_1^{d_1} \dots a_n^{d_n},$$

diremos que  $A$  é *finitamente gerada* sobre  $B$ . Esta condição é equivalente à existência de um homomorfismo sobrejetor  $B[\underline{X}] \longrightarrow A$  cuja restrição a  $B$  é a identidade  $B \longrightarrow B$ .

Esta situação será usada, principalmente, no caso em que  $B = k$ .

Dado um isomorfismo  $A \simeq B[\underline{X}]/J$  de  $B$ -álgebras (isto é, um isomorfismo de anéis cuja restrição a  $B$  é a identidade), diremos que a álgebra da direita é uma *apresentação* de  $A$  e que  $J$  é um *ideal de apresentação* de  $A$  sobre  $B$ .

**I.4 Estrutura dos ideais.** O conceito mais importante da teoria dos ideais e de suas aplicações é o de ideal primo.

(I.4.1) DEFINIÇÃO. Um ideal  $P \subset A$  é *primo* se, dados elementos  $a, b \in A$  tais que  $ab \in P$ , tem-se sempre  $a \in P$  ou  $b \in P$ .

Para evitar situações triviais, exigimos normalmente que um ideal primo  $P$  seja próprio, isto é, que  $P \neq A$ .

(I.4.2) EXEMPLOS. (i) O ideal gerado por um subconjunto de  $\underline{X}$  é um ideal primo em  $k[\underline{X}]$ .

(ii) O ideal gerado por um polinômio irredutível em  $k[\underline{X}]$  é um ideal primo.

Além dos magros exemplos acima e dos ideais em  $\mathbb{Z}$  gerados por números primos, não é tão fácil exibir outros. A verdade é que provar que um ideal,

dado por geradores explícitos, é primo é considerado um problema difícil – inclusive do ponto de vista de implementação computacional.

Uma noção mais fraca e, frequentemente, mais fácil de ser detectada é a seguinte.

(I.4.3) DEFINIÇÃO. Um ideal  $I \subset A$  é *radical* se  $I \neq A$  e se, dado  $a \in A$  tal que  $a^r \in I$ , para algum  $r \in \mathbb{N}$ , tem-se  $a \in I$ .

É claro que todo ideal primo é radical. Mostra-se que todo ideal radical é igual à interseção dos ideais primos que o contêm; em anéis razoáveis, – por exemplo, nas álgebras afins – todo ideal radical é uma interseção finita de ideais primos.

Esta decomposição pode ser vista como um caso particular de uma situação mais geral. Para tal, precisamos da seguinte noção.

(I.4.4) DEFINIÇÃO. Um ideal  $I \subset A$  é dito *primário* se, dados  $a, b \in A$  tais que  $ab \in I$ , então ou  $a \in I$  ou  $b^r \in I$ , para algum  $r \geq 0$ .

Em geral, incluímos na definição de um ideal primário  $I$  a hipótese de que  $I \neq A$ .

(I.4.5) FATO. (Decomposição primária de Noether) *Seja  $A$  uma álgebra afim sobre um corpo  $k$ . Todo ideal  $I \subset A$  admite uma decomposição como interseção finita*

$$(N) \quad \bigcap_i \Omega_i,$$

onde  $\Omega_i$  é um ideal primário.

Para dissecar (N), lembremos a noção de *radical* de um ideal  $I \subset A$ :

$$\text{rad } I := \{a \in A \mid a^r \in I \text{ para algum } r \geq 0\}.$$

Se  $\Omega$  é primário,  $\text{rad } \Omega$  é um ideal primo. Como a operação de passar ao radical comuta com a interseção de ideais, (N) diz que o radical de qualquer ideal é uma interseção finita de ideais primos. Estes primos dependem só de  $I$  e são chamados *primos mínimos* de  $I$  (ou de  $A/I$ ). O conjunto dos primos mínimos de  $A/I$  será denotado  $\text{Min } A/I$ .

A decomposição (N) não é única, mas pode ser simplificada, exigindo-se que  $\text{rad } \Omega_i \neq \Omega_j$  para  $i \neq j$ . Isto não impede a eventualidade de se ter  $\text{rad } \Omega_i \subsetneq \Omega_j$  para  $i \neq j$ .

(I.4.6) EXEMPLO.  $A = k[X, Y]$ ,  $I = (X^2, XY)$ . Uma decomposição primária de  $I$  é  $(X) \cap (X^2, J)$ , onde  $J \subset A$  é qualquer ideal contido em  $(Y)$ .

Este exemplo põe em evidência os seguintes fenômenos:

- (1) As componentes primárias em  $(N)$  não são unicamente determinadas pelo ideal;
- (2) Existem componentes primárias cujos radicais contêm propriamente o radical de alguma outra componente primária.

O radical de uma componente primária em  $(N)$ , que contém propriamente o radical de uma outra componente, é chamado primo *imerso* do ideal  $I$  (ou de  $A/I$ ). Em conjunto, primos mínimos e imersos constituem os primos *associados* do ideal  $I$  (ou de  $A/I$ ).

Esta noção pode ser recuperada de um outro ângulo.

(I.4.7) DEFINIÇÃO. Sejam  $I, J \subset A$  ideais. O *quociente* de  $I$  por  $J$  é o ideal

$$I : J = \{a \in A \mid aJ := \{ab \mid b \in J\} \subset I\}.$$

Observemos que sempre vale  $I \subseteq I : J$ , a igualdade podendo ter lugar em situação de “posição genérica” – por exemplo, se  $I$  é um ideal primo e  $J \not\subseteq I$ . Esta situação é especial, em geral acontecendo a inclusão própria.

(I.4.8) FATO. Um ideal primo  $P$  é um primo associado do ideal  $I$  se e só se existe um elemento  $a \in A \setminus I$  tal que  $P = I : (a)$ .

*Advertência:* Não é verdade, porém, que  $I : (a)$  seja sempre um ideal primo para qualquer escolha de  $a \in A \setminus I$ : é necessário, para tal, que  $a$  seja escolhido de tal maneira que o quociente  $I : (a)$  seja máximo entre os vários ideais desta forma.

**I.5 Anéis de frações.** Um subconjunto  $S \subset A$  de um anel  $A$  é chamado *multiplicativo* se for fechado sob a operação de multiplicação do anel.

Um conjunto multiplicativo  $S \subset A$  dá lugar à seguinte construção importante.

Introduzimos no conjunto  $A \times S$  dos pares uma relação de equivalência  $\equiv$  definida da seguinte maneira:

$$(a, s) \equiv (b, t) \Leftrightarrow \exists u \in S \mid u(at - bs) = 0.$$

Denotemos  $A_S$  (ou  $S^{-1}A$ ) o conjunto das classes de  $\equiv$ . A classe do par  $(a, s)$  será denotada  $a/s$ .

(I.5.1) DEFINIÇÃO. O anel de frações de  $A$  relativamente a (ou a denominadores em)  $S$  é o conjunto  $A_S$  munido das operações

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

Com estas operações,  $A_S$  é um anel e a aplicação  $\iota : A \rightarrow A_S$ , tal que  $\iota(a) = (as)/s$ ,  $s \in S$ , está bem definida e é um homomorfismo de anéis, chamado *estrutural*.

O homomorfismo estrutural  $\iota$  permite enunciar uma propriedade característica (ou universal) de  $A_S$ : para todo homomorfismo  $\varphi : A \rightarrow B$  tal que todo elemento de  $\varphi(S)$  admite inverso multiplicativo no anel  $B$ , existe um e um só homomorfismo  $\varphi_S : A_S \rightarrow B$  tal que  $\varphi_S \circ \iota = \varphi$ .

Normalmente, suporemos que  $1 \in S$ , de modo que  $\iota(a) = a/1$ . Observe-mos que  $\iota$  é injetora se e só se os elementos de  $S$  são elementos regulares de  $A$  (vide II.2 abaixo).

Eis os exemplos mais importantes (e os únicos que serão, possivelmente, usados no curso).

(I.5.2) EXEMPLOS. (i) (Localização num ideal primo) Se  $P \subset A$  é um ideal primo,  $S := A \setminus P$  é multiplicativo – a notação mais popular, neste caso, é  $A_P$ . O anel  $A_P$  é um exemplo de *anel local*, isto é, um anel que admite um único ideal máximo.

(ii) (Semi-localização) Generaliza (i): se  $P_1, \dots, P_m$  são ideais primos, então  $S := A \setminus \cup P_j$  é multiplicativo e o anel  $A_S = A_{P_1, \dots, P_m}$  é um exemplo de anel semi-local. Este anel é usado para definir as potências simbólicas de um ideal (vide *Palimpsesto 2*).

(iii) Para um elemento fixo  $a \in A$ , o conjunto das potências  $S_a := \{a^r | r \geq 0\}$  é multiplicativo. O anel  $A_S = A_a$  é muito útil em considerações ligadas à geometria algébrica.

## ANEIS E IDEAIS, II

### II.1 Teoria da dimensão.

(II.1.1) DEFINIÇÃO. A *altura* (ou *codimensão*) de um ideal primo  $P \subset A$  é o menor dos inteiros  $l$  para os quais existe uma cadeia

$$P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_l = P,$$

onde  $P_i$  é um ideal primo. A *altura* de um ideal arbitrário  $I \subset A$  se define como o mínimo das alturas dos seus ideais primos associados. Notação:  $\text{alt } I$ .

É claro, pela definição, que  $\text{alt } I = \text{alt } P$  para algum primo  $P \in \text{Min } A/I$ . Mas, primos mínimos distintos podem ter alturas diferentes.

(II.1.2) EXEMPLO.  $I = (XY, XZ) \subset k[X, Y, Z]$ . Tem-se  $\text{alt } I = \text{alt}(X) = 1$ , mas  $(Y, Z)$  também é um primo mínimo de  $I$ , de altura 2.

(II.1.3) DEFINIÇÃO. (Primeira forma da dimensão) A *dimensão* de um anel  $A$ , denotada  $\dim A$ , é o supremo das alturas dos seus ideais primos.

A definição é suficientemente geral para permitir patologias tais como anéis de dimensão infinita. Felizmente, tem-se:

(II.1.4) FATO. Se  $I$  é um ideal do anel  $k[\underline{X}]$ , tem-se

$$\dim k[\underline{X}]/I = \#\underline{X} - \text{alt } I \leq n < \infty.$$

Assim, álgebras afins têm dimensão finita.

Estas definições são de caráter combinatório. Contudo, a dimensão também admite uma versão mais geométrica. Para tal, nos restringiremos às álgebras afins.

(II.1.5) DEFINIÇÃO. Seja  $A = k[\underline{X}]/I$  uma álgebra afim graduada (isto é, o anel  $k[\underline{X}]$  é munido de uma tara de pesos  $(d_1, \dots, d_n)$  e  $I$  é quase-homogêneo relativamente a esta tara). Um *sistema de parâmetros (homogêneos)* de  $A$  é um conjunto de elementos homogêneos  $\theta_1, \dots, \theta_d$  tal que:

- (1)  $A/(\theta_1, \dots, \theta_d)$  é um  $k$ -espaço vetorial de dimensão finita;
- (2)  $d$  é o menor inteiro satisfazendo a propriedade (i).

(II.1.6) FATO. (Segunda forma da dimensão) Se  $A$  é uma álgebra afim graduada e se  $\theta_1, \dots, \theta_d$  é um sistema de parâmetros homogêneos, tem-se  $\dim A = d$ .

A álgebra afim padrão de dimensão  $d$  é, certamente, o anel de polinômios  $k[\underline{X}] = k[X_1, \dots, X_d]$ . Um teorema de *uniformização* (em geometria) é um resultado que permite relacionar, ao menos localmente, um objeto  $V$  de dimensão  $d$  com um objeto padrão  $V_0$  da mesma dimensão, através de uma



aplicação (chamada *uniformizante*)  $\pi : V \longrightarrow V_0$  que reflete as propriedades essenciais de  $V$ .

O teorema de uniformização algébrica é o ponto central da teoria das álgebras afins.

(II.1.7) FATO. (Teorema da normalização de Noether) *Seja  $A$  uma álgebra afim graduada sobre um corpo  $k$ . Então, existe um sistema de parâmetros homogêneos  $\theta_1, \dots, \theta_d$  de  $A$  tal que:*

- (i)  $k[\theta_1, \dots, \theta_d]$  é isomorfo ao anel de polinômios  $k[X_1, \dots, X_d]$ .
- (ii) Existem elementos  $\eta_1, \dots, \eta_m \in A$  tais que

$$A = \sum_{j=1}^m k[\theta_1, \dots, \theta_d]\eta_j.$$

(II.1.8) OBSERVAÇÃO. (i) O teorema admite uma versão não graduada.

(ii) A condição (i) do teorema significa que os elementos  $\theta_1, \dots, \theta_d$  são *algebricamente independentes* sobre o corpo  $k$ . Em verdade, pode-se mostrar que todo sistema de parâmetros é algebricamente independente.

(iii) A condição (ii) do teorema significa, na terminologia dos módulos sobre anéis, que  $A$  é um módulo finitamente gerado (pelos elementos  $\eta_1, \dots, \eta_m$ ) sobre o anel  $k[\theta_1, \dots, \theta_d]$  (vide III abaixo).

(II.1.9) DEFINIÇÃO. *Seja  $A$  uma álgebra afim contida num corpo. O grau de transcendência de  $A$  (sobre  $k$ ) é o máximo dos inteiros  $r$  para os quais existe um subconjunto de  $A$ , com  $r$  elementos, algebricamente independente.*

Notação:  $\text{gr. tr.}_k A$ .

O teorema de Noether admite então a seguinte variante.

(II.1.10) FATO. (Terceira forma da dimensão) *Se  $A$  é uma álgebra afim sobre  $k$ , tem-se  $\dim A = \text{gr. tr.}_k A$ .*

(II.1.11) OBSERVAÇÃO. *Se  $A$  não estiver contida num corpo, ainda vale que  $\dim A$  é o máximo dos cardinais dos subconjuntos algebricamente independentes sobre  $k$ .*

Finalmente, do teorema de Noether resulta:

(II.1.12) FATO. (Quarta forma da dimensão) *Seja  $A$  uma álgebra afim sobre  $k$  e seja  $I \subset A$  um ideal tal que  $\dim A/I = \dim A/P$  para todo  $P \in \text{Min } A/I$ . Então, tem-se*

$$\dim A = \dim A/I + \text{alt } I.$$

(II.1.13) DEFINIÇÃO. Um ideal  $I \subset A$  é de *dimensão pura* (ou, simplesmente, *puro*) se  $\dim A/I = \dim A/P$ , para todo primo associado  $P$  de  $A/I$ .

**II.2 Dimensão e profundidade.** Um elemento  $a \in A$  é *regular* (ou *não divisor de zero*) se  $ab = 0$ , com  $b \in A$ , implicar sempre em que  $b = 0$ . Um anel  $A$ , cujos elementos (com exceção de 0) são todos regulares, é chamado um *domínio de integridade* (ou um *domínio* ou ainda *um anel inteiro*).

Iterando a noção de elemento regular, temos uma das noções mais importantes da teoria.

(II.2.1) DEFINIÇÃO. Uma sequência de elementos  $a_1, \dots, a_r \in A$  é dita uma *A-sequência* (alternativamente, uma *sequência regular*), se o resíduo do elemento  $a_i$  no anel  $A/(a_1, \dots, a_{i-1})$  for regular, para todo  $1 \leq i \leq m$ .

(II.2.2) DEFINIÇÃO. A *profundidade* de um ideal  $I$  (ou, de  $A$  em  $I$ ) é o máximo dos cardinais das sequências regulares cujos elementos pertencem a  $I$ . Notação:  $\text{prof}_I A$ .

Se  $A = k[\underline{X}]/I$  é álgebra afim graduada, colocamos  $\text{prof } A := \text{prof}_{(\underline{X})} A$  e falamos, simplesmente, da *profundidade* de  $A$ .

(II.2.3) FATO. (i) Para todo ideal  $I \subset A$ , tem-se  $\text{prof}_I A \leq \text{alt } I$ .

(ii) Se  $A$  é afim graduado, vale  $\text{prof } A \leq \dim A$ .

A motivação central para este conceito e que norteia o curso, é dada pela seguinte.

(II.2.4) DEFINIÇÃO. Uma álgebra afim graduada  $A$  é de *Cohen-Macaulay* se  $\text{prof } A = \dim A$ .

(II.2.5) EXEMPLOS. (i) Um anel de polinômios  $k[\underline{X}]$  é um anel de Cohen-Macaulay, já que  $\underline{X}$  é uma sequência regular.

(ii) Para todo polinômio homogêneo  $f \in k[\underline{X}]$ , o anel de resíduos  $k[\underline{X}]/(f)$  é de Cohen-Macaulay.

(iii) Se  $k[\underline{X}]$  é munido de tara de pesos e  $f_1, \dots, f_r \in k[\underline{X}]$  é uma sequência regular de polinômios homogêneos relativamente à tara, então o anel  $k[\underline{X}]/(f_1, \dots, f_r)$  é de Cohen-Macaulay.

(iv)  $k[X, Y]/(X^2, XY)$  e  $k[X, Y, Z]/(XY, XZ)$  não são anéis de Cohen-Macaulay.

Uma das consequências importantes da propriedade é a pureza: se  $A = k[\underline{X}]/I$  é de Cohen-Macaulay, então o ideal  $I$  é puro.

Existe um bom número de caracterizações da propriedade de Cohen-Macaulay, dependendo do ângulo de interesse. Algumas destas foram reunidas na Proposição 4.1.2 do Capítulo 4. Uma caracterização muito útil é obtida a partir do teorema de normalização de Noether, substituindo-se a condição (ii) deste teorema pela seguinte: existem elementos  $\eta_1, \dots, \eta_m \in A$ , linearmente independentes sobre o subanel  $k[\theta_1, \dots, \theta_d]$  tais que

$$A = \sum_{j=1}^m k[\theta_1, \dots, \theta_d] \eta_j.$$

### III SUMÁRIO DE MÓDULOS

Um *módulo*  $M$  sobre um anel  $A$  é um grupo abeliano munido de uma operação de multiplicação por elementos de  $A$ , satisfazendo as propriedades usuais da definição de espaços vetoriais. Um *homomorfismo*  $M \rightarrow N$  é uma aplicação que preserva as duas operações estruturais.

Os módulos importantes, neste curso, são aqueles que admitem um conjunto finito de *geradores*, isto é um subconjunto  $\{\eta_1, \dots, \eta_m\} \subset M$  tal que  $M = \sum_{j=1}^m A\eta_j$ .

(III.1) EXEMPLOS. (i) O módulo padrão com  $m$  geradores é o *módulo livre*  $A^m = \sum_{j=1}^m Ae_j$ , onde  $e_j = (0, \dots, 0, \underset{j}{1}, 0, \dots, 0)$ .

(ii) Se  $A$  é um domínio, os submódulos de  $A^m$  (para os vários valores de  $m$ ) são os módulos *sem torção*. As sizíguas de um ideal, consideradas no Capítulo 4, Seção 4.6, habitam naturalmente estes módulos.

(iii) Um *módulo cíclico* é um da forma  $A/I$ , para algum ideal  $I \subset A$ , onde a multiplicação é induzida pela multiplicação estrutural do anel  $A$ .

(iv) Dados módulos  $M_1, \dots, M_s$ , a *soma direta*  $M_1 \oplus \dots \oplus M_s$  é definida da maneira usual, como sendo o conjunto das  $s$ -uplas com as operações coordenada a coordenada.

(v) Dado um  $A$ -módulo  $M$  e um  $A$ -submódulo  $N \subseteq M$ , definimos, por analogia com os anéis residuais, o *módulo residual* (ou *quociente*)  $M/N$ . Um caso particular importante é  $M/IM$ , obtido quando o submódulo é da forma  $IM$ , para um ideal  $I \subset A$

O *anulador* de um  $A$ -módulo  $M$  é o ideal

$$0 :_A M := \{a \in A \mid a\eta = 0, \forall \eta \in M\}.$$

(III.2) DEFINIÇÃO. A *dimensão* de um  $A$ -módulo  $M$  é  $\dim A/(0 :_A M)$ .

A noção de  $A$ -sequência se estende a módulos da seguinte forma. Um elemento  $a \in A$  é dito ser  *$M$ -regular* se o homomorfismo  $M \xrightarrow{a} M$  for injetor.

(III.3) DEFINIÇÃO. Dados um anel  $A$ , um ideal  $I \subset A$  e um  $A$ -módulo  $M$ , dizemos que uma sequência de elementos  $a_1, \dots, a_r \in I$  é uma  *$M$ -sequência em  $I$*  se, para todo  $1 \leq i \leq r$ , o elemento  $a_i$  for regular relativamente ao módulo quociente  $M/(a_1, \dots, a_{i-1})M$ .

A *profundidade de  $M$  em  $I$* , denotada  $\text{prof}_I M$ , é o máximo dos cardinais de  $M$ -sequências em  $I$ .

Como no caso de anéis graduados, para módulos que admitem uma graduação compatível com a graduação do anel  $A = k[\underline{X}]/I$ , a profundidade será tomada sempre relativamente ao ideal  $(\underline{X})/I$ .

A última noção a ser considerada é a seguinte.

(III.3) DEFINIÇÃO. Uma *sequência exata (curta)* de  $A$ -módulos é um par de homomorfismos  $\varphi : N \rightarrow M$  e  $\psi : M \rightarrow L$ , tais que

- (1)  $\varphi$  é injetor e  $\psi$  é sobrejetor.
- (2)  $\text{Nuc } \psi = \text{Im } \varphi$ .

Para indicar esta situação, usaremos o diagrama

$$0 \longrightarrow N \xrightarrow{\varphi} M \xrightarrow{\psi} L \longrightarrow 0.$$

O fato a seguir explica o comportamento da profundidade ao longo de uma sequência exata curta de módulos.

(III.4) FATO. Para todo ideal  $I \subset A$  e para toda sequência exata de  $A$ -módulos  $0 \rightarrow N \rightarrow M \rightarrow L \rightarrow 0$ , tem-se:

- (1) Se  $\text{prof}_I M > \text{prof}_I L$ , então  $\text{prof}_I N = \text{prof}_I L + 1$ .
- (2) Se  $\text{prof}_I M < \text{prof}_I L$ , então  $\text{prof}_I N = \text{prof}_I M$ .
- (3) Se  $\text{prof}_I M = \text{prof}_I L$ , então  $\text{prof}_I N \geq \text{prof}_I M$ .

## BIBLIOGRAFIA

- [ApHa77] K. Appel and W. Haken, *Every planar map is 4-colorable - 1: Discharging*, Ill. J. Math. **21** (1977), 429-490; *Every planar map is 4-colorable - 2: Reducibility*, Ill. J. Math. **21** (1977), 491-567.
- [Bac81a] K. Baclawski, *Rings with lexicographic straightening law*, Advances in Math. **39** (1981), 185-213.
- [Bac81b] —————, *Canonical modules of partially ordered sets*, Report, Insitut Mittag-Leffler No. **8** (1981).
- [BaGa81] K. Baclawski and A. M. Garsia, *Combinatorial decompositions of a class of rings*, Advances in Math. **39** (1981), 155-184.
- [Bay82] D. Bayer, *The division algorithm and the Hilbert scheme*, Ph.D. Thesis, Harvard, 1982..
- [BaMo89] D. Bayer and I. Morrison, *Standard Bases and Geometric Invariant Theory. I. Initial ideal and State Polytopes*, in "Computational methods of Commutative Algebra," (L. Robbiano, ed.), Academic Press, London San Diego New York, 1989, pp. 75-84.
- [BaSt87] D. Bayer and M. Stillman, *Macaulay, A computer algebra system for computing in algebraic geometry and commutative algebra*, 1986.
- [Bil82] L. J. Billera, *Polyhedral theory and commutative algebra*, in "Mathematical Programming - Bonn 1982, The State of the Art," (A. Bachem, M. Grötschel and B. Korte, eds.), Springer-Verlag, New York Heidelberg Japan, 1983.
- [Bre84] H. Bresinsky, *Minimal free resolutions of monomial curves in  $\mathbb{P}^3$* , Linear Algebra and Appl. **59** (1984), 121-129.
- [Brø83] A. Brøndsted, "An Introduction to Convex Polytopes," Graduate Texts in Mathematics, Springer, New York, 1983.
- [BrMa71] H. Bruggesser and P. Mani, *Shellable decompositions of cells and spheres*, Math. Ann. **29** (1971), 197-205.
- [BrRe80] H. Bresinsky and B. Renschuch, *Basisbestimmung Veronesescher Projektionideale mit allgemeiner Nullstelle*, Math. Nachr. **96** (1980), 257-269.
- [BrSiTr91] W. Bruns, A. Simis and N. V. Trung, *Blow-up of straightening-closed ideals in ordinal Hodge algebras*, Trans. Amer. Math. Soc. (to appear).
- [BrSiVa88] P. Brumatti, A. Simis and W. Vasconcelos, *Normal Rees algebras*, J. Algebra **112** (1988), 26-48.
- [BrVe88] W. Bruns and U. Vetter, "Determinantal rings," Lecture Notes in Mathematics Vol. **1327** (Subseries: IMPA, Rio de Janeiro), Springer, Berlin-Heidelberg-New York, 1988.
- [Buc65] B. Buchberger, *Ein algorithmus zum Auffindem des Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomidealen*, Dissertation, Universität Innsbruck.
- [Buc85] *Gröbner bases: an algorithmic method in polynomial ideal theory*, in "(N. K. Bose, ed.) Multidimensional Systems Theory," D. Reidel Publishin Co., 1985, pp. 184-232.

- [CaNi] M. P. Cavaliere and G. Niesi, *On monomial curves and Cohen-Macaulay type*, Manuscripta Math. **42** (1983), 147–159.
- [Cay889] A. Cayley, *A theorem on trees*, Quart. J. Math. **23** (1889), 376–378.
- [CILI69] G. Clements and B. Lindström, *A generalization of a combinatorial theorem of Macaulay*, J. Combinatorial Theory **7** (1969), 230–238.
- [Coo71] S. A. Cook, *The complexity of theorem-proving procedures*, in “Proc. 3rd ACM Symp. on Theory of Computing,” Associatio for Computing Machinery, New York, 1971, pp. 151–158.
- [Cow85] C. Cowsik, *Symbolic powers and number of defining equations*, in “Algebra and its Applications,” Lecture Notes in Pure and Applied Mathematics Vol **91**, Marcel Dekker, New York, 1985, pp. 13–14.
- [CoEiPr82] C. de Concicni, D. Eisenbud and C. Procesi, *Hodge algebras*, Astérisque **91** (1982).
- [Dan78] V. I. Danilov, *The geometry of toric varieties*, Russian Math. Surveys **33** (1978), 97–154; Uspekhi Math. Nauk **33** (1978), 971–982.
- [DeKuRo78] J. Désarménien, J. Kung and G. C. Rota, *Invariant theory, Young bitableaux, and combinatorics*, Advances in Math. **27** (1978), 63–92.
- [DoRoSt74] P. Doubilet, G. C. Rota and J. Stein, *On the foundation of combinatorial theory: IX. Combinatorial methods in invariant theory*, Stud. Appl. Math. **53** (1974), 185–216.
- [Eli83] S. Eliaouhu, *Courbes monomiales et algèbre de Rees symbolique*, Thèse No. 2080, Université de Genève.
- [Er61] P. Erdős, *The theory of graphs and probabilities, II*, Can. J. Math. **13** (1961), 346–352.
- [EwSh74] G. Ewald and G. C. Shephard, *Stellar subdivisions of boundary complexes of convex polytopes*, Math. Ann. **210** (1974), 7–16.
- [Fro82] R. Fröberg, *A study of graded extremal rings and of monomial rings*, Math. Scand. **51** (1982), 22–34.
- [Fru38] R. Frucht, *Herstellung von Graphen mit vorgegebner abstrakte Gruppe*, Compositio Math. **6** (1938), 239–250.
- [GaJo76] M. R. Garey and D. S. Johnson, *Approximation algorithms for combinatorial problems: an annotated bibliography*, in “(J. F. Traub (ed.)) Algorithms and Complexity: New Directions and Recent Results,” Academic Press, New York, 1976, pp. 41–52.
- [GaJo78] \_\_\_\_\_, *Strong NP-completeness results: motivation, examples and implications*, J. Assoc. Comput. Mach. **25** (1978), 499–508.
- [GaJo79] \_\_\_\_\_, “Computers and Intractability,” A guide to the theory of NP-completeness, W. H. Freeman and Co., New York, 1979.
- [Gar80] A. M. Garsia, *Combinatorial methods in the theory of Cohen-Macaulay rings*, Advances in Math. **38** (1980), 229–266.
- [Gav72] F. Gavril, *Algorithms for minimum coloring, maximum clique, minimum covering by cliques, and maximum independent set for a chordal graph*, SIAM J. Comput. **1** (1972), 180–187.

- [GeKaZe89] I. M. Gelfand, M. M. Kapranov and A. V. Zelevinsky, *Newton polytopes of principal A-determinants*, Doklady AN SSSR **308** (1989), 20–23.
- [Grü67] B. Grünbaum, “Convex Polytopes,” Interscience, New York, 1967.
- [GrSt91] P. Gritzmann and B. Sturmfels, *Minkowski addition of polytopes: computational complexity and applications to Gröbner bases*, preprint, 1991..
- [Har72] F. Harary, “Graph theory,” Addison-Wesley Series in Mathematics, Addison-Wesley, Reading, Mass., 1972.
- [HaPa73] F. Harary and E. M. Palmer, “Graphical Enumeration,” Academic Press, New York, 1973.
- [Her26] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788.
- [HeSiVa83] J. Herzog, A. Simis and W. Vasconcelos, *Koszul homology and blowing-up rings*, in “Commutative Algebra,” Proceedings: Trento 1981 (S. Greco and G. Valla, Eds.), Lecture Notes in Pure and Applied Math., Marcel Dekker, New York, 1983, pp. 79–169.
- [Hoc72] M. Hochster, *Rings of invariants of tori, Cohen–Macaulay rings generated by monomials, and polytopes*, Ann. Math. **96** (1972), 318–337.
- [HoPe52] W. V. D. Hodge and D. Pedoe, “Methods of Algebraic Geometry,” Vol. II, Cambridge University Press, Cambridge, 1952.
- [HuSiVa89] C. Huneke, A. Simis and W. Vasconcelos, *Reduced normal cones are domains*, in “Proceedings of an AMS Special Session: Invariant Theory (Eds. R. Fossum, M. Hochster and V. Lakshmibai),” Contemporary Mathematics, American Mathematical Society, Providence, RI, 1989.
- [Kar72] R. M. Karp, *Reducibility among combinatorial problems*, in “R. E. Miller and J. W. Thatcher (eds.), Complexity of Computer Computations,” Plenum Press, New York, 1972, pp. 85–103.
- [KaStZe91] M. M. Kapranov, B. Sturmfels and A. V. Zelevinsky, *Chow polytopes and general resultants*, preprint, 1991.
- [Kle64] V. Klee, *A combinatorial analogue of Poincaré duality theorem*, Can. J. Math. **16** (1964), 517–531.
- [Knu70] D. E. Knuth, *Permutations, matrices and generalized Young tableaux*, Pac. J. Math. **34** (1970), 709–727.
- [Kru35] W. Krull, “Idealtheorie,” Ergebnisse, Springer, Berlin, 1935.
- [Lov67] L. Lovász, *On chromatic number of finite set-systems*, Acta. Math. Acad. Sci. Hungar. **79** (1967), 59–67.
- [Lyu88] G. Lyubeznik, *On the arithmetical rank of monomial ideals*, J. Algebra **112** (1988), 86–89.
- [Mac27] F. S. Macaulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. **26** (1927), 531–555.
- [MaMe82] E. Mayr and A. Meyer, *The complexity of the word problem for commutative semigroups and polynomial ideals*, Adv Math. **46** (1982), 305–329.
- [McM70] P. McMullen, *The maximum number of faces of a convex polytope*, Mathematika **17** (1970), 179–184.

- [McSh71] P. M. McMullen and G. C. Shephard, "Convex Polytopes and the Upper Bound Conjecture," Lecture Notes Series, London Mathematical Society, 1971.
- [Moo67] J. Moon, *Enumerating labelled trees*, in "Graph theory and theoretical physics," Academic Press, New York, 1967.
- [MoRo89] T. Mora and L. Robbiano, *The Gröbner fan of an ideal*, in "Computational methods of Commutative Algebra (L. Robbiano, ed.)," Academic Press, London San Diego New York, 1989, pp. 49–74.
- [MoSi90] M. Morales and A. Simis, *Symbolic powers of monomial curves lying on  $xw - yz$* , preprint, 1990.
- [MoSi91] M. Morales and A. Simis, *The second symbolic power of an arithmetically Cohen-Macaulay monomial curve in  $\mathbb{P}^3$* , preprint, 1991.
- [Mot57] T. S. Motzkin, *Comonotone curves and polyhedra*, Abstract 111, Bull. Amer. Math. Soc. **63** (1957), 35.
- [Mun86] J. Munkres, *Topological results in combinatorics*, Michigan Math. J. **31** (84), 113–128.
- [Oda78] T. Oda, "Lectures on Torus Embeddings and Applications," (Based on joint work with K. Miyake) Tata Inst. of Fund. Research **58**, Springer, Berlin Heidelberg New York, 1978.
- [Oda88] ———, "Convex Bodies and Algebraic geometry," *Ergebnisse der Mathematik und ihrer Grenzgebiete, Series 3*, Vol. **15**, Springer, Berlin Heidelberg New York, 1988.
- [Ost21] A. Ostrowski, *Über die Bedeutung der Theorie der konvexen Polyeder für die formale Algebra*, Jahresberichte Deutsche Mat. Verein. **30** (1921), 98–99.
- [Ost75] ———, *On multiplication and factorization of polynomials, I. Lexicographic orderings and extreme aggregates of terms*, Aequationes Math. **13** (1975), 201–228.
- [Pet891] J. Petersen, *Die Theorie der regulären Graphen*, Acta Math. **15** (1891), 193–220.
- [Ree56] D. Rees, *A basis theorem for polynomial modules*, Proc. Cambridge Philos. Soc. **52** (1956), 12–16.
- [Rei76] G. Reisner, *Cohen–Macaulay quotients of polynomial rings*, Advances in Math. **21** (1976), 30–49.
- [Rob89] L. Robbiano, *Gröbner bases: a foundation for Commutative Algebra*, preprint, 1989.
- [Sch61] C. Schensted, *Longest increasing and decreasing subsequences*, Can. J. Math. **13** (1961), 179–191.
- [Sch89] P. Schenzel, *Examples of Gorenstein domains and symbolic powers of monomial space curves*, preprint, 1989.
- [Sim90] A. Simis, *Topics in Rees algebras of special ideals*, in "Commutative Algebra, Proceedings: Salvador 1988 (Eds. W. Bruns, A. Simis)," Lecture Notes in Mathematics Vol. **1430**, Springer-Verlag, Berlin Heidelberg New York London Paris Tokyo, 1990, pp. 98–114.
- [Sim91] ———, *On graphs and ideals*, Preliminary draft, 1991.



- [SiVaVi91] A. Simis, W. Vasconcelos and R. Villarreal, *The ideal theory of graphs*, in preparation.
- [Spe30] E. Sperner, *Über einen kombinatorischen Satz von Macaulay und seine Anwendung auf die Theorie der Polynomideale*, Abh. Math. Sem. Univ. Hamburg **7** (1930), 149–163.
- [Sta79] R. Stanley, *Balanced Cohen-Macaulay complexes*, Trans. Amer. Math. Soc. **249** (1979), 139–157.
- [Sta83] ———, “Combinatorics and Commutative Algebra,” Progress in Mathematics, Birkhäuser, 1983.
- [StRa34] E. Steinitz and H. Rademacher, “Vorlesungen über die Theorie der Polyeder,” Springer, Berlin, 1934.
- [Stu90a] B. Sturmfels, *Gröbner bases and Stanley decompositions of determinantal rings*, Math. Z. **205** (1990), 137–144.
- [Stu90b] ———, *Gröbner bases of toric varieties*, preprint, 1990.
- [StWh89] B. Sturmfels and N. White, *Gröbner bases and Invariant Theory*, Adv. Math. **76** (1989), 245–259.
- [StWh90] ———, *Computing combinatorial decompositions of rings*, Combinatorica (to appear).
- [SiUIVa90] A. Simis, B. Ulrich and W. V. Vasconcelos, *Jacobian dual fibrations*, preprint, 1990.
- [Tem64] H. N. V. Temperley, *On the mutual cancellation of cluster integrals in Mayer’s fugacity series*, Proc. Phys. Soc. **83** (1964), 3–16.
- [Vil90] R. Villarreal, *Cohen-Macaulay graphs*, Manuscripta Math. **66** (1990), 277–293.
- [Whi28] F. Whipple, *On a theorem due to F. S. Macaulay*, J. London Math. Soc. **8** (1928), 431–437.

## A

Álgebra, 37-39.  
   afim, 130.  
   Comutativa, 37, 42, 60, 85.  
   dimensão de, 134.  
   discreta, 39.  
   finitamente gerada, 38, 130.  
   fundamental, 89-91, 93, 96, 98.  
   de Hodge, 37-39.  
   de Hodge ordinal, 97-99.  
   de Rees, 87-90, 96, 98, 116-117.  
   de Rees estendida, 99.  
   simétrica, 87-88, 93.  
 Algoritmo, 115.  
   de Buchberger, 116.  
   determinístico, 122.  
   não determinístico, 122.  
 Altura, 47, 50.  
 Anel, 37-39.  
   das arestas, 45-46.  
   de Cohen-Macaulay, 44, 60-61,  
     63-64, 66, 68, 71-72, 75-78, 82.  
   determinantal, 43, 96.  
   das faces, 45, 51.  
   de frações, 109, 132-133.  
   graduado, 40-41, 43-44, 56, 58,  
     60-63, 82, 87.  
   de Petersen, 46-49, 76-77, 79, 82.

  de polinômios, 38, 39-40.  
   de resíduos, 129.  
   de Stanley-Reisner, 1, 4, 69.  
 Aresta, 2-6, 9, 14-15, 20, 48-49.  
   contração de, 48.  
   grafo-, 30.  
 Árvore, 4, 6, 8-10, 17, 20, 22, 30-32,  
   50, 83.  
   de Cohen-Macaulay, 83.  
   enraizada, 21.  
   geradora, 8-9.  
   suspensão de, 83.  
   uniramada, 21-22.  
 Automorfismo, 6-8.  
   de um grafo, 6-8.  
   grupo de, 6.

## B

Baricêntrica, 33.  
   divisão, 33, 45, 68.  
 Base, 37, 55.  
   de Gröbner, 43, 95-96, 105-106,  
     114-115, 119.  
   vetorial, 38, 41, 53.  
 Bipartido, 6, 32.  
   grafo, 6, 19-20, 92, 95.  
 Bi-tabela, 42.  
   básica ("standard"), 42.

## 2 INDICE REMISSIVO

- comprimento de, 42.
- Booleano, modelo, 124.
- variáveis, 123–124.

### C

- Caminho monomial, 91–92.
- Ciclo, 6, 8–9, 17, 20–22, 81.
  - ímpar, 6, 107, 11–113.
  - gerador, 8–9.
- Cobertura, 14.
  - mínima, 14–19, 46–47, 51.
  - número de, 15.
  - de vértices, 14–16, 46, 123.
  - vetor de (de primeira ordem), 17.
- Cohen–Macaulay, 39, 44, 60, 76.
  - anel, 39, 44, 60–61, 63–64, 66, 68, 71–72, 75, 78, 82.
  - complexo, 64–67, 69, 72, 75.
  - complexo duplamente de, 80.
  - grafo, 76, 79–81, 82–83.
  - grafo criticamente de, 80–81.
- Cohomologia, 70–72.
- Coloração, 9–10.
  - de vértices, 9–10.
- Complexidade, 9, 14, 22, 120, 125.
  - arbórea, 9.
  - NP-completo, 14, 122–123, 125.
  - temporal, 121.
- Complexo, 11.
  - de cadeias, 33, 66.
  - de Dehn–Sommerville, 74.
  - dimensão de, 23.
  - equilibrado, 24.
  - esqueleto de, 23.
  - face de, 23.
  - grafal, 31, 33–34, 45, 56.
  - homologia de, 69–70, 71–73.
  - $h$ -vetor de, 64–65.
  - puro, 24.
  - simplicial, 11, 22–28, 31–32, 51–56, 64–66, 70, 72, 74–75, 80.
  - realização poliédrica de, 26, 65, 70, 72, 75.
- Computação, 114.
  - algébrica, 114–116.
  - simbólica, 115.
- Conexo, 5, 80, 82, 92.
  - grafo, 112.
- Conjunto,
  - multiplicativo, 132–133.
  - parcialmente ordenado, 10–12.
  - parcialmente ordenado catenário, 10.
- Conjetura,
  - da cota superior, 73–75.
  - da cota inferior, 75.
- Construtível, 65–66.

Corda, 33, 93.  
 Córdico, 34, 126.  
 Cromático,  
   número, 10, 112–113.  
   polinômio, 10.

## D

Decomposição,  
   de Hironaka–Rees, 43–44, 68.  
   primária, 131.  
 Diagrama de Hasse, 12, 32, 98.

## E

Elo, 23, 72.  
 Envoltória,  
   afim, 25, 29.  
   convexa 25–26, 118.

## F

Face, 23.  
   anel de, 45, 51.  
   elo de, 23, 72.  
   estrela de, 23.  
 Fecho,  
   inteiro, 118.  
 Função de Hilbert, 54, 56–58, 61–63.

Funtorialidade,  
   do anel de Petersen, 48–50.  
   do anel de Stanley–Reisner, 54.  
*f*-vetor, 18.  
   de um complexo simplicial, 55–56,  
     64–65.  
   de um politopo, 27–29.

## G

Grafo, 2–10.  
   álgebra de, 90.  
   aresta de, 2–6.  
   –aresta, 30.  
   cinto de, 113.  
   complementar, 31, 112.  
   completo, 4, 7, 10, 14, 17, 92–95.  
   hamiltoniano, 8.  
   isomorfismo de, 3, 6.  
   morfismo de, 3, 49.  
   multiplicidade de, 79.  
   pedestal de, 82–83.  
   puro, 14.  
   realização de, 2–6.  
   realização poliédrica de, 5.  
   realização retilínea de, 5.  
   subgrafo gerador de, 8.  
   subgrafo induzido de, 49.  
   tipo de, 82.

vértices de, 2.

## H

Homologia, 69.

bordo de, 69.

cadeia de, 69.

ciclo de, 69.

simplicial, 69.

singular, 70.

Homomorfismo, 48-50.

de anéis, 128-129.

## I

Ideal, 39-40, 128-129.

altura de, 47, 133.

de apresentação, 89.

das arestas, 46.

de ordem, 10-11, 37, 39, 41, 96.

de Petersen, 46.

primário, 131.

primo, 47, 96, 130.

primo mínimo, 47, 77, 96, 131.

quociente de, 132.

radical, 46, 94, 131.

de tipo linear, 88, 92.

Inersão, 3-4.

geométrica, 3.

Independência,

complexidade de, 82-83.

número de, 19.

Independente,

algebricamente, 53, 86, 135.

analiticamente, 86.

conjunto, 18-22.

linearmente, 37, 42, 99, 137.

Isomorfismo,

de grafos, 3.

de anéis, 128.

## L

Leque, 107.

de Gröbner, 108.

normal, 107-108.

Local,

anel, 133.

estimativa, 50.

Localização, 50, 133.

## M

Monômio, 36-41, 44, 51-53.

básico ("standard"), 37-38, 99.

fatoração básica, 67-68.

fôrma, 67-68.

indivisível, 37, 98-99.

livre de quadrados, 36, 70.

peso de, 40.

semigrupo de, 40.

suporte de, 52–53, 67.

Módulo, 137–138.

anulador de, 137.

cíclico, 137.

geradores de, 137.

homomorfismo de, 137.

residual, 137.

sequência exata de, 138.

Multicadeia, 10.

Multiplicidade, 78–79.

de um anel, 78.

de um grafo, 79.

## N

Normalização, teorema de, 111, 135.

NP, 122.

–completo, 14, 122–123, 125.

## O

Ordem,

lexicográfica, 40.

parcial, 10.

de termos, 41, 105.

total 40–41.

## P

P, 122.

Partição, 9–10, 19, 24.

ramada, 21–22.

Pedestal, 82–83.

Permutaedro, 104.

Politopo, 25–29, 73–75.

cíclico, 26–27, 73–74.

cone poliédrico de, 107.

dimensão de, 25.

de estado, 104.

face de, 25.

faceta de, 27, 65.

fronteira de, 65, 75.

$f$ -vetor de, 27–29.

–matroide, 104, 106.

de Newton, 104.

simplicial, 26, 28–29, 75.

Potência simbólica, 108–112, 118–120.

Profundidade, 60, 66, 136, 138.

Pseudo-potência, 56.

## R

Relação, 84.

algébrica, 84, 90.

linear, 84, 93–94.

## 6 INDICE REMISSIVO

polinomial, 84, 88.

de retificação, 37, 97.

Residual, 129.

ancl, 46, 52, 129.

módulo, 137.

Resíduo, 41, 43-44, 51-53.

## S

Segre, variedade de, 89, 102.

Sequência,

$A$ -, 60-61.

exata, 66, 138.

$h$ -, 57-58, 63-65.

monomial léxica, 57-58

regular, 85-86.

Série,

de Hilbert, 55, 60-65.

de Hilbert fina, 71.

de Laurent, 71.

Simbólica,

computação, 115.

índice, 111-113.

potência, 108-112, 118-120.

variável, 116.

Sistema de parâmetros, 60-61, 63, 69,

79, 81, 134-135.

Soma de Minkowski, 106.

Suspensão de um grafo, 76-77, 79-80,  
82-83.

## T

Termo, 36, 39-41.

inicial, 106.

largura de, 42.

Tipo, 82, 93.

Tipo linear, ideal de, 88.

Toro algébrico, 101-102.

## V

Valência de um vértice, 6.

Variedade,

determinantal, 103.

de Grassmann, 104.

de Segre, 89, 102.

tórica, 101-103.

de Veronese, 89, 102.

Vértice, 2.

de um grafo, 2-6.

de um complexo simplicial, 11, 22.

grau de, 6.

## Z

Zonotopo, 107.

Impresso no Setor de  
Reprografia do  
Inst. de Matemática e Coppe  
U F R J